A Brief survey on Intrusion Detection System for WSN

L.Sheeba, Dr.V.S.Meenakshi

Research Scholar, Research Supervisor & Department of Computer Science, Chikenna Government Arts College & Bharathiar University
Tamilnadu, India

Abstract— *Wireless Sensor Networks (WSNs) are the collection of autonomous sensor nodes spread out in various hostile environments statically or dynamically depend upon the application to monitor temperature, sound, pressure, etc. The security is a major component in wireless sensor networks. It degrades the performance of the network. The intrusion detection system is the solution to detect different kinds of attacks occurring on sensor nodes.Wireless sensor networks (WSN) are a group of tiny devices. These tiny devices have few energy, computational power, transmission range and memory. The more modern networks are bi-directional, also enabling control of sensor activity. At the beginning wireless sensor networks was developed for military applications such as battlefield surveillance; nowadays such networks are mostly used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. WSN has been used in many applications such habitat monitoring, building monitoring, smart grid and pipeline monitoring. Intrusion detection model takes advantage of cluster-based architecture to reduce energy consumption. This model uses anomaly detection based on support vector machine (SVM) algorithm and a set of signature rules to detect malicious behaviours and provide global lightweight IDS. Though a few restricted survey works on this topic have already been done but there is a great need of performing a detailed study on the vital aspects so that the IDS is analyzed in all the different angles. Three most intrusion detection techniques explored in this paper. Such as Anomaly detection, Misuse detection and Specification based detection. Here in this review paper various attacks on Wireless Sensor Networks and existing Intrusion detection techniques are discussed to detect the compromised node/s.*

Keywords— *IDS, DOS, Anomaly Detection.*

I. INTRODUCTION (SIZE 10 & BOLD)

Wireless Sensor Networks (WSNs) have grown to become one of the most promising and interesting fields over the past few years. WSNs are wireless networks consisting of distributed sensor nodes that cooperatively monitor physical or environmental conditions. A sensor node is a tiny and simple device with limited computational resources. Sensor nodes are randomly and densely deployed in a sensed environment.

A. Types of Intrusion Detection Systems

Intrusion detection is defined as real-time monitoring and analysis of network activity and data for potential Vulnerabilities and attacks in progress. One major limitation of current intrusion detection system (IDS) technologies is the requirement to filter false alarms lest the operator (system or security administrator) be overwhelmed with data. IDSs are classified in many different ways, including active and passive, network-based and host-based, and knowledge-based and behaviour-based:

- Active and passive IDS
- Network-based and host-based IDS
- Knowledge-based and behavior-based IDS

B. Active and passive IDS

An **Active IDS** (now more commonly known as an intrusion prevention system — IPS) is a system that's configured to automatically block suspected attacks in progress without any intervention required by an operator. IPS has the advantage of providing real-time corrective action in response to an attack but has many disadvantages as well. An IPS must be placed in-line along a network boundary; thus, the IPS itself is susceptible to attack. Also, if false alarms and legitimate traffic haven't been properly identified and filtered, authorized users and applications may be improperly denied access. Finally, the IPS itself may be used to effect a Denial of Service (DOS) attack by intentionally flooding the system with alarms that cause it to block connections until no connections or bandwidth are available.

A **passive IDS** is a system that's configured only to monitor and analyse network traffic activity and alert an operator to potential vulnerabilities and attacks. It isn't capable of performing any protective or corrective functions on its own. The major advantages of passive IDSs are that these systems can be easily and rapidly deployed and are not normally susceptible to attack themselves.

A **Network-Based IDS** usually consists of a network appliance (or sensor) with a Network Interface Card (NIC) operating in promiscuous mode and a separate management interface. The IDS is placed along a network segment or boundary and monitors all traffic on that segment.

A **Host-Based IDS** requires small programs (or agents) to be installed on individual systems to be monitored. The agents monitor the operating system and write data to log files.

Knowledge-based and behavior-based IDS:

A **knowledge-based** (or signature-based) IDS references a database of previous attack profiles and known system vulnerabilities to identify active intrusion attempts. Knowledge-based IDS is currently more common than behavior-based IDS.

A **Behavior-Based** (or statistical anomaly–based) IDS references a baseline or learned pattern of normal system activity to identify active intrusion attempts. Deviations from this baseline or pattern cause an alarm to be triggered.

Intrusion Detection: Techniques:

- ✓ Misuse detection systems
- ✓ Anomaly detection systems
- ✓ Specification-based detection

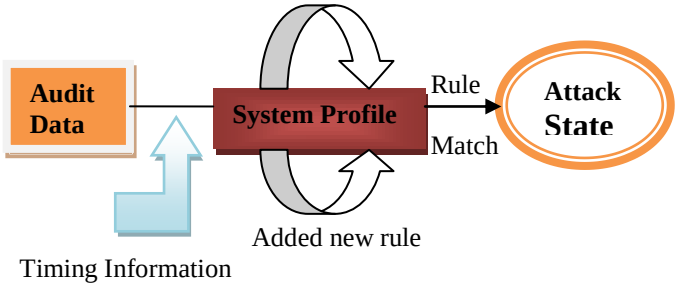

Fig. 1 Misuse Detection Systems

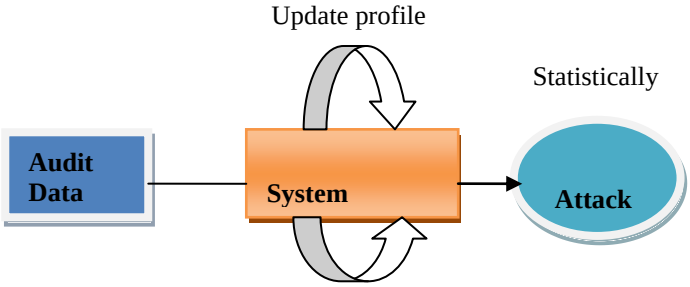

Fig. 2 Anomaly Detection Systems

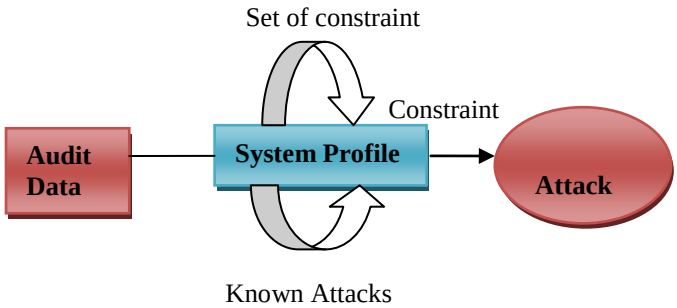

Fig. 3 Specification based detection

C. Classification

Classification of intrusion detection systems. The main reason is that many of them are based on more than just one approach and could implement a number of methods. Some systems could use different techniques on different levels of information processing. They could also run in different operation modes under different configuration parameters. The author describes in this paper thinks that it is more correct to talk about classification of IDS functional and operational characteristics, rather than about classification of IDS itself [31].The following figure summarizes classifications that could be found in information sources on intrusion Detection.

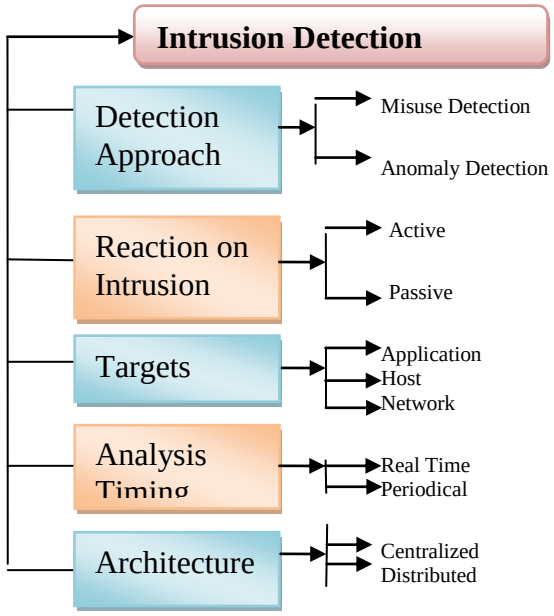

Fig. 4 IDS characteristics classification

It gives a brief explanation of characteristics shown in the figure. As they already said before, IDS could be based on one of two previously described approaches: misuse detection or anomaly detection.

IDS can react to detected intrusion in two ways. When it takes some actions (like closing holes, shutting services down, logging an intruder) as a reaction to the intrusion, such IDS is called active. If it just generates some alarms or notifications, it is called passive.

Detect intrusions at the application level. For instance, it could be a Web- or e-commerce server. Host-based IDS (sometimes called agents or sensors) collect and analyze information on activity on a certain host in the system. Network-based IDS operate on the network level and analyze the network traffic.

Audit information analysis can be done generally in two modes. Intrusion detection process can run continuously, also called in real-time. The term "real-time" indicates not more than a fact that IDS reacts to an intrusion "quick enough". Intrusion detection process also can be run periodically.

Another quite interesting characteristic of IDS is its architecture. Tendencies of intrusion detection systems development follow the same way as computer systems development. Traditional IDS are centralized. It means that they are implemented either as a one monolithic module or a

number interacting ones, which inherit the overall IDS functionality. Now it is said more and more often about fully distributed IDS that consist of entities, which are distributed over a system and each of them carries its own task. It is very important to point once again out, that we are talking here not about the physical distribution of IDS components, but about its functionality distribution.

TABLE 1

EXISTING MODEL	ATTACK USED	DETECTION TECHNIQUE	HIGHLIGHTING FEATURES
Chris Karlof *, David Wagner ELSEVIER - Ad Hoc Networks 1 2003	Novel Attacks	Using LEACH to Form Hierarchical Clusters.	Routing Protocol to Violate the Security Goals
Md. Safiqul Islam *1, Syed AshiqurRahman*2-IJAST 2011	Malicious Attacks, Network Attacks	Prevention based and detection based	Cooperative detection engine.
Hossein Jadidoleslamy IJNSA 2011	Malicious Attacks	Decision Tree (DT) With Data Mining Technique.	Provide a new framework for security scheme to integrate access control
Han Zhijie, Wang Ruchuang ELSEVIER -2012	Selective Forwarding Attacks, DOS Attacks.	Prevention based Techniques and detection based techniques.	To determine better node features addressing specific vulnerabilities and to develop improved detection algorithms with sensor node capabilities in mind
H.H. Soliman a, Noha A. Hikal b, Nehal A. Sakr b,*- Egyptian Informatics Journal -2012	Anomalous Attacks	Hybrid detection techniques and Statistical-based techniques.	Extracted from each traffic flow.
Sumit More, Mary Matthews, Anupam Joshi, Tim Finin - IEEE 2012	Cyber Attacks, 8070 attacks	NS Simulator.	Experiment With Integration Of Newer Data Sources.
Karen A. Garc´ıa, Ra´ul Monroy, Luis A. Trejo, Carlos Mex-Perera, and Eduardo Aguirre - IEEE Transactions- 2012	Mimicry Attacks	System-Based Intrusion Detection Specification-Based Intrusion Detection Learning-Based Intrusion Detection	The mechanism much more robust, although this is a rather challenging task.
Djallel Eddine Boubiche1 and Azeddine Bilami2 – IJNSA 2012	Detecting More Complex Attacks	NS Simulator.	Approach doesn't claim to be immune from all security attacks
Joseph Rish Simenthy CEng , AMIE, K. Vijayan, IJCSCE- 2012	Detecting More Complex Attacks	MATLAB	IDS is imposed on both homogenous and heterogeneous WSN model
Abror Abduvaliyev, Al-Sakib Khan Pathan, Jianying Zhou, Rodrigo Roman, and Wai-Choong Wong - IEEE Communications -2013	Security Attacks, Novel Attacks, Sinkhole/Black hole attacks.	Misuse detection, Anomaly detection, Specification-based detection	Prove the effectiveness of the different IDS mechanisms

Salvatore Pontarelli, Giuseppe Bianchi, and Simone Teofili- IEEE Transactions- 2013	Detect New Emerging Attacks	Ant evasion Techniques	Best Implementations of the Five SMEs(String Match Engine)
Robert Mitchell and Ing-Ray Chen, Member, IEEE Transactions- 2013	Black hole and Grey hole Attacks	Anomaly detection, specification-based detection	Able to detect attackers While limiting the false positive probability to protect the continuity Of operation is of utmost importance.
Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, Member, IEEE Transactions -2013	Malicious Attacks	Hybrid cryptography techniques	Testing the performance of EAACK in real network environment instead of software simulation.
Emad Felemban- Scientific Research- 2013	-------	WSN border surveillance techniques	High spatial and temporal data resolution
Sushma J. Gaurkar, Piyush K.Ingole - International Journal Of Scientific & Technology Research- 2013	Malicious attacks.	Decision Tree (DT) With Data Mining Technique.	It will explore high level decision tree construction in base station and detection of unknown attack.
Robert Mitchell and Ing-Ray Chen - IEEE Transactions - 2014	Malicious Attacks.	Behavior-Rule Based Intrusion Detection Technique	Detection Rate Without Compromising the False Positive Probability.
Ismail Butun, Salvatore D. Morgera, and Ravi Sankar- IEEE Communications Surveys- 2014	Black hole and selective forwarding attacks, Active and passive Attacks.	Prevention,Detection,Mitigation	Scalable, fast intrusion detection.
Weiming Hu, Jun Gao, Yanguo Wang, Ou Wu, and Stephen Maybank- IEEE Transactions On Cybernetics- 2014	Block Network Attacks.	IDS Simulator	IDSs are distributed on network, installed in common nodes.
Robert Mitchell, Ing-Ray Chen- ELSEVIER -2014	Cyber Attacks, Dos Attacks.	UAV intrusion Detection technique.	The shortcomings of MANET simulations and emulations.
Joseph Rish Simenthy CEng, AMIE, K. Vijayan – IJAREEIE- 2014**.**	Security Attacks	Anomaly detection based detection	It improves the detection rate and efficiency so that almost all the Intrusions can be detected.
Omar Said1,3*† and Alaa Elnashar2,3 - EURASIP Journal on Wireless Communications and Networking -2015	DOS Attacks	Prevention Technique	WSN is recommended in 3D environments.
Anush Ananthakumar,Tanmay Ganediwal,Dr. Ashwini Kunte, IJACSA-2015	Multiple Anomaly Attacks	Signature Based, Anomaly Based And Hybrid Based	Countermeasures which are faster and more effective

III. RESEARCH AND DISCUSSION

In [1] Chris Karlof [*], David Wagner, proposed IDS to analyze the security of security of sensor network by using sinkhole and hello floods,these techniques are vulnerable to blackmailers.

In [2] HanZhijie, Ruchuang, developed traffic based IDS in Wireless Sensor Network.The technique markov model are used to find the performance with better false alarm rate.

In [3] H.H. Soliman [a], Noha A. Hikal [b], etal, they evaluates the strength and weakness of wireless sensor network and it experimental result are compared with Support Vector Machine.

In [4] Sumit More, etal proposed IDS to detect cyber threats Or vulnerabilities in Wireless Sensor Network.

In [5] Karen A etal, in this paper, proposed a novel approach for postmortem intrusion detection experimental result compared with K-means to detect the cumulative detection rate over 90%.

In [6] Abror Abduvaliyev etal, Produced recent advancement in Wireless Sensor Network research area to predict and to identify the research challenges.

In [7] Salvatore Pontarelli etal, this work, proposed to promote different traffic-aware modular approach to design FPGA based NIDA.The system helps to reduce 80% real world traffic problems.

In [8] Robert Mitchell etal, developed behavior rule based IDS for physical devices to detect the intrusion among them.

In [9] Elhadi M. Shakshuki, proposed anew enhanced adaptive acknowledgement (EAACK) Intrusion Detection for MANETS and it compare with several techniques.

In [10] Emad Felemban, presented a survey of current experimentation and research work done in border surveillance applications.

In [11] Robert Mitchell and Ing-Ray Chen, developed IDS to detect malicious attacks in airborne system using behavior rule based IDS Techniques.

In [12] Ismail Butun etal, In this article, presented a survey of different kinds of IDS used in Mobile Ad-hoc Networks and also it highlighted open research issues in that field.

In [13] Weiming Hu etal, developed a online Ad- Boost based intrusion detection algorithms using PSO and SVM based algorithm.

In [14] Robert Mitchell etal, presented a survey to identify gaps and research direction in wireless Network IDS and also it summarize lof of IDS Techniques and suggesation to the future researchers.

In [15] Omar Said[1, 3*†] and Alaa Elnashar[2, 3†], developed a new model for 3D wireless sensor network. It constructed using OPNET and NS2.To find better performance in evaluating approaches.

In [16] Hossein Jadidoleslamy, design questionnaire to verify the proposed system. It was derived from the 50 experts people of WSN.

In [17] Sushma J. Gaurkar, Piyush K.Ingole, proposed a framework for intrusion Detection at sensor with access control. The new framework is used to integrate access control with include low-level intrusion detection.

In [18] Namita Singh ,Uday Singh , proposed to monitor intrusion activities and realize abnormal process in local nodes with effective energy consumption using agent-based intrusion detection to detect the DOS attacks for self recovery system.

In [19] Joseph Rish Simenthy CEng , AMIE, K. Vijayan, developed to detect rate and efficiency to almost all intrusion can be detected .This advanced intrusion detection system is applicable for all type of networks with wide range of flexibility.

In [20] Djallel Eddine Boubiche[1] and Azeddine Bilami[2] , proposed a new intrusion based on the interaction of the network.NS is used to demonstrate different types of attacks and a model with new direction toward WSN security.

In [21] Jasvinder Singh[1], Er. Vivek Thapar[2], developed to product the tight security for deployment area. To identify how the intruders reach confidential area to detect the probability of intruders.

In[22]Md. Safiqul Islam[*1],Syed AshiqurRahman[*2] ,proposed work is to identify the security threats and how they are implemented in intrusion Detection.

In [23] Anush Ananthakumar, Tanmay Ganediwal, Dr. Ashwini Kunte, presented a survey to identify counter measures with ever-growing attacks to improve network protection.

In [24] Hossein Jadidoleslamy, proposed a sensor based IDS to design and deploy a cluster based intrusion detection's with wide range of WSN.

In [25] Ms R. khewale etal, proposed work is to extend the life of WSN.IDS create cluster based wireless sensor network to find better sensor nodes and it proves effectiveness of simulated environment.

In [26] S.Yamunarani, D.Sathya, paper discussed different types of techniques used to improve accuracy and reduce false positive rate.

In [27] Vijay Bhuse paper discussed with identify a new type of attack and analyzing with the unifying frame work of intrusion detection light weight solutions.

In [28] Tapolina Bhattasali [1], Rituparna Chaki [2] , proposed work focus on layer to find the counter measure with great efficiency using MATLAB.

In [29] Michael Krishnan, paper focus on new game theoretic approach in which packets were determines. To increase energy and resource of network.

In [30] Ana Paula R etal, proposed work is to identify different kinds of simulated attacks to find the restrictions of networks.

IV.CONCLUSION

In this survey paper, IDSs along with their classification, design specification and requirement. On basis of this survey work, the proposed algorithm Our IDS uses a learning algorithm based on the SVM and several detection techniques. Such as misuse, anomaly, signature based detection based on the attacks. Indeed, the combination of these techniques to offers an intrusion detection system with high detection rate and false positive rate. Finally, in order to help researchers in the selection of IDS for WSN recommendation of promising proposed schemes are provided along with future direction for this research work.

REFERENCES

[1]. Chris Karlof [*], David Wagner, Secure routingin wireless sensor networks: attacks and countermeasures, Elsevier - Ad Hoc Networks 1 (2003) 293–315.

[2].HanZhijie, Ruchuang, Intrusion Detection for Wireless Sensor Network Based on Traffic Prediction Model, Elsevier -2012 International Conference on Solid State Devices and Materials Science, Physics Procedia 25 (2012) 2072 – 2080.

[3]. H.H. Soliman [a], Noha A. Hikal [b], Nehal A. Sakr [b,*], A comparative performance evaluation of intrusion detection techniques for hierarchical wireless sensor networks, Egyptian Informatics Journal (2012) 13, 225–238.

[4]. Sumit More, Mary Matthews, Anupam Joshi, Tim Finin , A Knowledge-Based Approach To Intrusion Detection Modeling, IEEE Symposium on Security and Privacy Workshops 2012, 75 -81.

[5]. Karen A. Garc´ıa, Ra´ul Monroy, Luis A. Trejo, Carlos Mex-Perera, and Eduardo Aguirre, Analyzing Log Files for Postmortem Intrusion Detection, IEEE transactions on systems, man, and cybernetics—Part C: Applications and Reviews, Vol. 42, No. 6, November 2012, 1690-1704.

[6]. Abror Abduvaliyev, Al-Sakib Khan Pathan, Jianying Zhou, Rodrigo Roman, and Wai-Choong Wong, On the Vital Areas of Intrusion Detection
Systems in Wireless Sensor Networks, IEEE Communications Surveys & Tutorials, Vol. 15, No. 3, Third Quarter 2013, 1223-1237.

[7]. Salvatore Pontarelli, Giuseppe Bianchi, and Simone Teofili, Traffic-Aware Design of a High-Speed FPGA Network Intrusion Detection System, IEEE Transactions On Computers, Vol. 62, No. 11, November 2013 , 2322- 2334.

[8]. Robert Mitchell and Ing-Ray Chen, Member, IEEE, Behavior-Rule Based Intrusion Detection Systems for Safety Critical Smart Grid Applications, IEEE Transactions On Smart Grid, Vol. 4, No. 3, September 2013, 1254- 1263.

[9]. Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, Member, IEEE, EAACK—A Secure Intrusion-Detection

System for Manets, IEEE Transactions On Industrial Electronics, VOL. 60, NO. 3, MARCH 2013, 1089- 1098.
[10].Emad Felemban, Advanced Border Intrusion Detection and Surveillance Using Wireless Sensor Network Technology, Int. J. Communications, Network and System Sciences, 2013, 6, 251-259.
[11]. Robert Mitchell and Ing-Ray Chen, Adaptive Intrusion Detection of Malicious Unmanned Air Vehicles Using Behavior Rule Specifications, IEEE Transactions On Systems, Man, And Cybernetics: Systems, Vol. 44, No. 5, May 2014, 593-04.
[12]. Ismail Butun, Salvatore D. Morgera, and Ravi Sankar, A Survey of Intrusion Detection Systems in Wireless Sensor Networks, IEEE Communications Surveys & Tutorials, Vol. 16, No. 1, First Quarter 2014,266-282.
[13]. Weiming Hu, Jun Gao, Yanguo Wang, Ou Wu, and Stephen Maybank, Online Adaboost-Based Parameterized Methods for Dynamic Distributed Network Intrusion Detection, IEEE Transactions On Cybernetics, Vol. 44, No. 1, January 2014 ,66-82.
[14]. Robert Mitchell, Ing-Ray Chen *, Review A survey of intrusion detection in wireless network applications, Elsevier Computer Communications 42 (2014) 1–23.
[15]. Omar Said[1,3*†] and Alaa Elnashar[2,3†,] Scaling of wireless sensor network intrusion detection probability: 3D sensors, 3D intruders, and 3D environments, EURASIP Journal on Wireless Communications and Networking (2015) ,1-12.
[16]. Hossein Jadidoleslamy, A Hierarchical Intrusion Detection Architecture For Wireless Sensor Networks, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011, 131-154.
[17]. Sushma J. Gaurkar, Piyush K.Ingole, Access Control And Intrusion Detection For Security In Wireless Sensor Network, International Journal Of Scientific & Technology Research Volume 2, Issue 6, June 2013 ISSN 2277-8616,63-67.
[18]. Namita Singh,Uday Singh, Intrusion Detection And Self-Recovery System, Namita Singh et al , International Journal of Computer Science & Communication Networks,Vol 4(3),111-118 111 ISSN:2249-5789,111-118.
[19].Joseph Rish Simenthy CEng , AMIE, K. Vijayan, Advanced Intrusion Detection System for Wireless Sensor Networks, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, An ISO 3297: 2007 Certified Organization Vol. 3, Special Issue 3, April 2014, 167- 172.
[20].Djallel Eddine Boubiche[1] and Azeddine Bilami[2] , Cross Layer Intrusion Detection System For Wireless Sensor Network, International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012,35-52.
[21].Jasvinder Singh[1], Er. Vivek Thapar[2], Intrusion Detection System in Wireless Sensor Network, International Journal of Computer Science and Communication Engineering Volume 1 Issue 2 (December 2012 Issue), ISSN: 2319-7080, 76-80.
[22]. Md. Safiqul Islam [*1], Syed AshiqurRahman[*2], Anomaly Intrusion Detection System in Wireless Sensor Networks: Security Threats and Existing Approaches, International Journal of Advanced Science and Technology Vol. 36, November, 2011,1-8.
[23]. Anush Ananthakumar, Tanmay Ganediwal, Dr. Ashwini Kunte, Intrusion Detection System in Wireless Sensor Networks: A Review, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 6, No. 12, 2015, 131-139.
[24]. Hossein Jadidoleslamy, A High-Level Architecture for Intrusion Detection on Heterogeneous Wireless Sensor Networks: Hierarchical, Scalable and Dynamic Reconfigurable, scientific Research Wireless Sensor Network, 2011, 3, 241-261.
[25]. Miss R. khewale; Miss M. Ramteke; Miss D. Bawane;Miss S. Tathe, Miss T. padmagiriwar, A Survey on Hybrid Intrusion Detection of Cluster- Based Wireless Sensor Network, International Journal Of Research In Advent Technology Vol.3 No.2, February 2015,E-ISSN: 2321-9637,164-167.
[26]. S.Yamunarani, D.Sathya, A Survey on Intelligent Intrusion Detection System in Wireless Sensor Networks, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 1, January 2015,80-84.
[27]. Vijay Bhuse, Student Member, IEEE, Ajay Gupta, Senior Member, IEEE and Leszek Lilien, Senior Member, IEEE, Research challenges in lightweight intrusion detection for wireless sensor networks, Research challenges in lightweight intrusion detection for wireless sensor networks 1-6.
[28]. Tapolina Bhattasali [1], Rituparna Chaki [2], A Survey of Recent Intrusion Detection Systems for Wireless Sensor Network, 1-10.
[29]. Michael Krishnan, Intrusion Detection in Wireless Sensor Networks, 1-7.
[30]. Ana Paula R. da Silva Marcelo H.T. Martins Bruno P.S. Rocha Antonio A.F. Loureiro Linnyer B. Ruiz Hao Chi Wong, Decentralized Intrusion Detection in Wireless Sensor Networks, 2005, 16-23.
[31]. Mikhail Gordeev, Intrusion Detection: Techniques and Approaches
[32]. Swati Kasar, Trupti Wagh, A Survey on Intrusion Detection Techniques in Wireless Sensor Networks, International Journal of Computer Applications (0975 – 8887) National Conference on Emerging Trends in Advanced Communication Technologies (NCETACT-2015