ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 3, Special Issue 3, April 2014*

International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy (ICSECSRE '14)

Organized by

Department of ECE, Aarupadai Veedu Institute of Technology, Vinayaka Missions University,

Paiyanoor-603 104, Tamil Nadu, India

Advanced Intrusion Detection System for Wireless Sensor Networks

Joseph Rish Simenthy CEng , AMIE, K. Vijayan

Dept. of Telecommunication and Networks, SRM University, Kattankulathur,Tamil Nadu, India

Abstract— Wireless Sensor Network consists of large number of nodes which will be in distributed nature. Security is a very important consideration while designing a Wireless Sensor Network. So an Avanced Intrusion detection System has been proposed where the Hybrid Intrusion Detection System(HIDS), Energy Prediction based Intrusion Detection System (EPIDS) as well as the Cross layer Detection System are implemented In various stages in order to assure maximum possible security from the Intrusions. Energy Prediction Approach alone is not suitable for the WSN, so HIDS which is suitable for large and sustainable WSN's is combined. Also combining these two approaches along with the Cross Layer IDS make it suitable for a large WSN also. So the new proposed IDS will offer a wide range of flexibility for its application in any type of Wireless Sensor Networks.

Keywords– Wireless Sensor Network, Intrusion Detection System, HIDS,EPIDS ,Cross layer ,Nodes ,Energy Efficiency

I. INTRODUCTION

Wireless Sensor Network is a new technology which is becoming more popular and useful in many areas like Military application, Environmental monitoring, Home application, Health or medical application, Industrial monitoring, Structural strength monitoring etc.[10] Over the years, it has been emerged as a competent technology. WSN has a group of sensor nodes which are deployed over the area of application and provided with energy sources for its efficient working. Sensor nodes differs in their characteristics like separation distance, energy level etc based on the application area. In other words we can say that they are application dependent. Also WSNs are vulnerable to many types of security attacks. This is because of transmission medium's broadcast nature. Also WSNs have additional vulnerability because nodes are placed in areas prone to physical attacks or hostile environment.

Many security solutions for WSNs have been proposed , they are authentication, key exchange, and secure routing. These are only capable of ensuring security upto certain level. These cannot detect or eliminate all the security attacks. So an Intrusion Detection System (IDS) is considered as the foremost solution to address wide range of security problems. Almost all IDSs can only detect the attacks or intrusions[3]. They cannot prevent them or eliminate them. An Intrusion is termed as an unauthorised or unlawful activity which is carried out by the external agents in order to harm the network resources or the sensor nodes. So as discussed earlier an IDS will detect such activities. The main function of the IDS are to keep an eye on the user's activities and network behaviour at different layers. No IDS is capable of giving a perfect solution for the intrusions. So a combination of 2 or more IDSs are found to be effficient. So in order to achieve a perfect defence from the intrusions , different IDSs should be employed at different levels in order to meet the accuracy.[8]

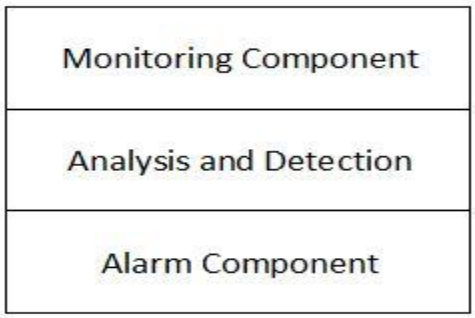

Fig- 1

There are 2 basic classes of IDSs called as signature based IDSs and anomaly based IDS [9] . In signature based IDS , the signature or properties of different security attacks are maintained in the database. The IDS is very effective in

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 3, Special Issue 3, April 2014*

International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy (ICSECSRE '14)

Organized by

Department of ECE, Aarupadai Veedu Institute of Technology, Vinayaka Missions University,

Paiyanoor-603 104, Tamil Nadu, India

the case of wellknown security attacks but when new security attacks arises, the detection rate is very low because th signaatures are not included in the database. In the case of anomaly based IDS, it detects the new IDS but misses the well known attacks. Anomaly based IDS will maintain any signatures in the database because they continuously keeps an eye on traffic pattern or the system activities.

This paper is organized as follows. Section II describe the details of the related work, section III describes the Advanced Intrusion Detection System. Section IV simulation results. Section V conclusion of the work.

II. RELATED WORK

WSNs have limited computation, Bandwidth, memory, and energy. They uses multihop communication strategy and are distributed in nature. The limitation will be taken into considration while designing any proposal for WSN. Due to hostile environment, security becomes the major problem. IDSs has the ability to detect an intrusion and raise an alarm for taking appropriate action[12]. Due to the enegy and computational power limitation, designng appropriate IDS for WSN is a challenging task.

A Hybrid intrusion Detection System (HIDS) [1] is acombination of Signature based as well as the anomaly – based IDSs. It not only has the advantages of both the IDSs. It has their limitations too. Both well known as well as new intrusions or attacks can be detected using this. So it works well compared to the Signature based or the Anomaly- based IDSs [9] used separately. But the disadvantage is that only a few type of intrusions will be detected. When it comes to a large network where the intrusions are internal as well as external, HIDS seems to be less benefitial. So there is a high probabilty that the IDS may fail.So in order to avoid this the new proposed IDS will combine other two types of IDSs along with the HIDS namely Energy Prediction based Intrusion Detection System and Cross Layer Intrusion detection System. This makes the new IDS more powerful and efficient.

Physical Layer of the WSN is responsible for radio and signals management[8]. One of the most severe attack is Radio Jamming. The other Physical Layer attack is battery exhaustion attack. The battery power is an important factor which plays an important role and determines the lifetime of the network. So keeping in view the power limitation of the WSN's, it is desirable to design power efficient mechanism for sustainable WSNs. The attacker will not allow the sensor nodes to switch to sleep mode in energyexhaustion attack. In sleep mode the sensor nodes will consume less energy.

In energy exhaustion attack, unnecessary data or becons will be sent intermittently the sensor nodes and keeps it always busy[2]. Also as it is deployed in hostile environment, many physical attacks such as battery replacement,node destruction, replacement of nodes, replication of nodes and node reprogramming with a malicious code will be affected.So the Energy Prediction based Intrusion Detection System (EPIDS) will calculate the initial energy of the nodes and the consumption rate for the normal functioning of the nodes will be preprogrammed. Any Consumption rate other than this will be indicated by the IDS. But this IDS has limitations as the consumption rate of the energy by the nodes may be varied according to other parameters too. Intrusions may not be always the reason.

Combining the methodologies of Cross Layer IDS may be found benefitial in this case. The working principle of a Cross layer IDS may be discussed as follows. A WSN will be divided in to different clusters [6] having a cluster head and other cluster members. The different steps which are implemented in this IDS are, firstly a list of suspected nodes will be foundout by estimating the attacked area. Inconsistency in the data can be found by the base station by using the statistical method described as follows.

Let X_1……..X_n be the sensing data collected. Let X be the mean. Then,

$$F(X_j)= \sqrt{((X_j- X)^2/x)}$$

If X_j is greater than a threshold value, a node become suspicious, because the date from this particular node will be different from other nodes. So pthe poition of sink hole is estimated by the base station, which circles a particular attacked area, which contains all the suspected nodes. The radius of the circle will be chosen so that it will cover almost all the suspected nodes. In the second phase of the Cross layer IDS, the intrusion will be identified by analaysing the routing pattern in the area which is affected. A request message which contains the ID's of all the affected nodes will be broadcasted by the base station. A time stamp will be also included in a request signed with the private key of the base station to prevent replay attacks. The node which is affected replies with its own ID, the ID of the next hop node and the routing cost to

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 3, Special Issue 3, April 2014*

International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy (ICSECSRE '14)

Organized by

Department of ECE, Aarupadai Veedu Institute of Technology, Vinayaka Missions University,

Paiyanoor-603 104, Tamil Nadu, India

that node on receiving the request. A reply message will be sent along the reverse path in the broadcast, as the next hop and the routing cost will be affected by the attack.

All network traffic flow towards the same destination which discloses the intruders identity in a sink hole attack. In this case the power consumption significantly reduces as the IDS doesnot require communication between the sensor nodes. Also a wide range of routing attacks can be detected. The properties and functioning of the various IDSs can be summarised as follows. Thus combining these IDSs , we will get an efficient system which can detect almost all the intrusions. The disadvantages of the IDSs when used alone can be avoided in this case.[5][8][11]

Characteristics	Anomaly Based	Signature Based	Hybrid	Cross layer	Energy Prediction Based
Detection Rate	Medium	Medium	High	High	High
False Alarm	Medium	Medium	Low	Low	Low
Computation	Low	Low	Medium	High	High
Energy Consumption	Low	Low	Medium	High	Low
Attack Detection	Few	Few	More	More	More
Multi layer Attack detections	No	No	No	Yes	No
Strength	Capable of detecting new attacks	Detects all those attacks having signatures	Can detect both existing and new attacks	Can detect multilayer attacks	Can detect and recognize malicious attacks effectively
Weakness	Misses well known attack	Cannot detect new attacks	Requires more computation and resources	Requires more resources	only considers the energy consumption of particular node
Suitable for WSN	Yes	Yes	With Justification	With strong Justification	With Strong Justification

Fig- 2

III. ADVANCED INTRUSION DETECTION SYSTEM

In this IDS, the combination of Enenrgy Prediction based IDS, Hybrid Intrusion Detection System as well as the Cross Layer IDS will be implemented. This will be done in different stages, which is discussed as follows

A. Cluster Head Selection

As the WSN consists of different nodes, the cluster head selection is an important procedure in this IDS, The algorithm is as follows:[7]

S_i – Set of type i sensors in the WSN area.
S- Set of all sensors in the network.
N(a)- Set of neighbours of node a.
Repeat
For i=1 to N
Select node a with min N(a) in Set S_i
If $N(a) \neq \phi$
Select a
SN= { j/the distance between a and N(a)< (r_{si}/2) }
If SN>1
S=S-(SN U a)
Else
S=S-a
Until S is null set

In this way the cluster head will be formed. The cluster head will be having the maximum amount of energy as compared to the other sensor nodes. As energy consumption rate is the main consideration here for the evalution of the performance of the Advanced Intrusion Detection System.

B. Working Principle

After the cluster head has been selected, the sensor nodes will be communicating with the cluster head. The cluster heads communicate with each other. The energy consumption rate of the sensor nodes when they are attacked will be different from the normal working condition[4]. That means the security attacks causes the sensor nodes to consume more energy. So which ever node consuming more power will be affected. In this way using the Energy Prediction System where the normal energy consumption rate will be calculated and will be compared with the present condition where the sensor node is affected by the attack. This gives the clear evidence that the node is affected and will be continuously monitered till another performance variation is detected.

The most common attacks such as Selective Forwarding Attack, Worm Hole Attack, Sybil Attack, Sink Hole Attack, Hello Flood Attack etc [9] has a predefined energy consumption rate and that means if the present Energy Consumption rate matches with any of these the IDS will clearly find out the attack and gives a clear cut indication. Fig-3 shows the graph in which the energy consumption rate vs Denial of Service attacks is given. So from this the attacks energy consumption behaviour can be clearly understood.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 3, Special Issue 3, April 2014*

International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy (ICSECSRE '14)

Organized by

Department of ECE, Aarupadai Veedu Institute of Technology, Vinayaka Missions University,

Paiyanoor-603 104, Tamil Nadu, India

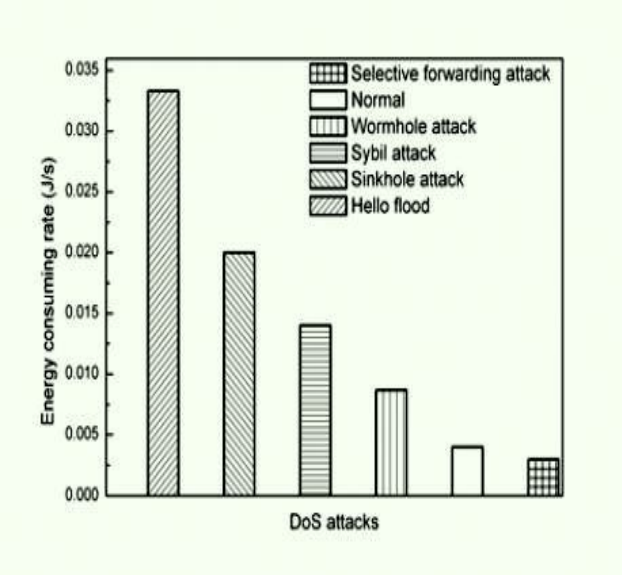

Fig- 3

Problem arises when the energy consumption of the sensor nodes increase with the internal problems itself [7]. If the battery of a sensor node is in a faulty condition due to the physical damage, it will show variation in the energy consumption or dissipation rate. So the IDS will assume that there is an intrusion and will start giving indication for that. So the Energy Prediction System alone cannot be employed for the efficient detection of the Intrusions. So the Hybrid Intrusion Detection System will be employed at the next level. The sensor nodes which showed abnormal Energy consumption rate will be checked for the Intrusions again using the Hybrid Intrusion Detection System , which is a combination of Signature based as well as the Anomaly based Intrusion detection Systems.

As discussed earlier the Signature based IDS will check for the well known attacks and the Anomaly based IDS will check for the new attacks. So if an attack is found it will go through the next evaluation step , that is Cross Layer IDS. Also if the nodes which are not found to be faulty will be removed from the black list. It will continue its normal working after being corrected for its error which may be due to the physical damage.

The current Intrusion Detection up to this level will detect almost all the attacks. But there is limitation when it comes to the attacks occuring between the OSI layers. Also a combination system which had Energy Prediction based as well as the Hybrid IDSs will work efficietly for small or medium sized wireless Sensor Networks. For a large network with many number of sensors, it will not be suitable. So we use the cross Layer IDS also along with it. So the combination of the three IDSs will clearly detect all the possible Intrusions with high degree of accuracy. So the proposed IDS called as the Advanced Intrusion Detection System is not only capable of detecting almost all the Intrusions but also applicable to small, medium and large sized Wireless Sensor Networks.

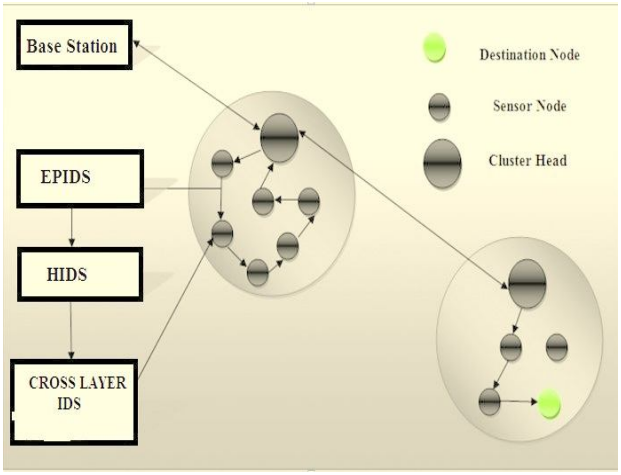

Fig- 4

Fig 4 shows the principle of Advanced Intrusion Detection System in detail. There are two groups of nodes as shown in bigger circles. Inside the circular group, there are sensor nodes located. The bigger ones are the cluster heads .

IV. PERFORMANCE EVALUATION

A test bed was created in JAVA using the NetBeans editor. A virtual Wireless Sensor Network was created with N number of nodes randomly. And according to the proposed algorithm and the energy level of the nodes, the cluster head was selected. Now the IDSs were performed in various levels. But in order to claim that the proposed IDS was perfect, there is a need to compare the performance of the current system with the existing ones.Fig- 5 clearly shows the Delivery Ratio vs Percentage of affected nodes. In this case The Hybrid Intrusion Detection System as well as the Energy Prediction

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 3, Special Issue 3, April 2014*

International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy (ICSECSRE '14)

Organized by

Department of ECE, Aarupadai Veedu Institute of Technology, Vinayaka Missions University,

Paiyanoor-603 104, Tamil Nadu, India

Based Intrusion Detection System was compared with the proposed Advanced Intrusion Detection System.

In this graph the red line shows the performance of the Hybris Intrusion Detection System, the blue line shows the Energy Prediction based Intrusion Detection System and the green line shown the proposed Advanced Intrusion Detection System. It is clearly recognisable from the graph that the performance of the nergy prediction system is very low when the percentaage of the affected nodes increases. That means, the delivery radio gragually decreases to a very low level when the percentage of affected nodes increases. So we cannot rely on the Energy Prediction based system alone. The red line which shows the Hybrid Intrusion detection system shows better performance compared to the Energy prediction based System. When it comes to the Advanced Intrusion detection system, the performance is far better than the Energy Prediction based Intrusion Detection System and fairly better than the Hybrid Intrusion Detection System.

So from the performance graph we can conclude that the proposed system gives better results than the Energy Prediction Based Intrusion Detectiion System and the Hybrid Intrusion Detection System. Thus when the percentage of affected nores increases the Advanced Intrusion Detection System gives better results.

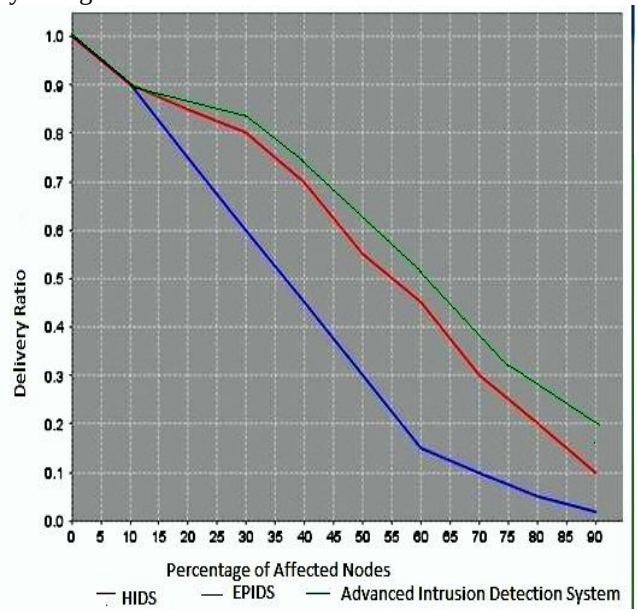

Fig-5

Next we compared all the systems such as the Energy Prediction Based IDS, Hybrid IDS, Cross Layer IDS etc with the Advanced Intrusion Detection System. The primary aim was to get the detection probability rate. That means how much effective the proposed system was compared to the existing three systems. Also we wanted to know the false positive probability too. So a graph was plot Detection probability vs False Positive probability and the performance of the four IDS was compared. This is clearly shown in the Fig- 6.

Here in the graph, the red line shows the Energy prediction Based Intrusion Detection System, the blue line shows the Hybris Intrusion Detection System, the black line shows the Cross layer Intrusion detection system and the green line shows the Advanced Intrusion detection system. From the graph we can analyse that the Energy prediction based system gives more false positives and the detection probability is low. In the case of Cross layer IDS, the performance is far more better. The Hybrid IDS gives far more better results that the Energy prediction based and the Cross Layer IDSs. The Proposed system gives a far more stable result as compared to the existing three IDSs.

So we can clearly conclude from the comparison graphs Delivery Ratio vs Percentage of Affected Nodes and Detection probability rate vs False positive probability that, the Advanced Intrusion Detection System gives better results. It also improves the energy efficiency and there by the system life time also will be greatly increased. Also it is applicable to small, medium as well as large sized networks.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 3, Special Issue 3, April 2014*

International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy (ICSECSRE '14)

Organized by

Department of ECE, Aarupadai Veedu Institute of Technology, Vinayaka Missions University,

Paiyanoor-603 104, Tamil Nadu, India

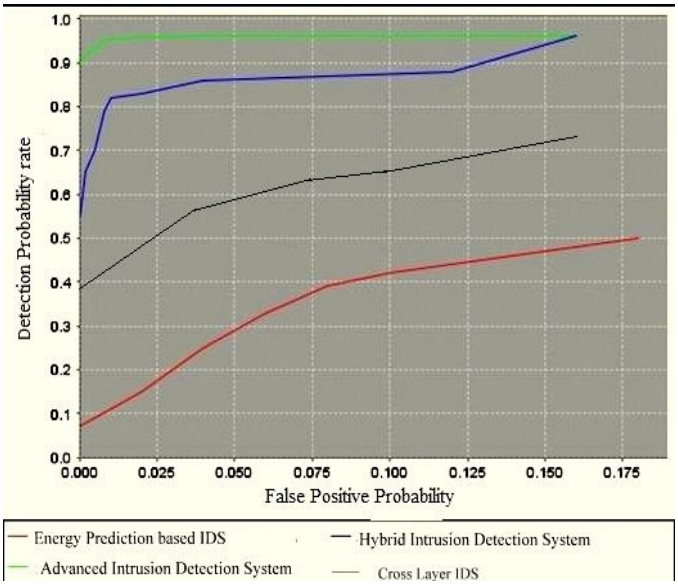

Fig- 6

V.CONCLUSION

We know that security is the main criteria while designing a Wireless Sensor Network. Due to the Broadcast nature of the medium, they are more prone to security attacks. In this paper, an Advanced Intrusion Detection System has been proposed. It improves the detection rate and efficiency so that almost all the Intrusions can be detected. Also the system is applicable to Small , medium as well as large sized networks. That means it gives a wide range of flexibility in detection of Intrusions compared to the other existing systems. Also the energy efficiency and the system life time is greatly improved.

REFERENCES

[1.] 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 NETWORKS*", COMPUTER SCIENCE AND INFORMATION TECHNOLOGY(ICCSIT),3RD IEEE INTERNATIONAL CONFERENCE,9-11 JULY 2010

[2.] Wen Shen, Guangjie Han,Lei Shu, joel Rodrigues and Naveen Chilamkurti," *A New Energy Prediction Approach for Intrusion Detection in Cluster-Based Wireless Sensor Networks*",Green Communications and Networking, Springer,Volume 51,pp 1-12,2012

[3.] Yun Wang, Bin Xie and Dharma P. Agrawal , "*Intrusion Detection in Homogeneous and Herogeneous Wireless Sensor Networks*", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 7, NO. 6, JUNE 2008 , 698-711,2008 21-23

[4.] A.Shakil Ahmed, Dr.A.Rajeswari **"***Intrusion Detection in Heterogeneous Wireless Sensor Networks With an Energy Efficient Localization Algorithm"* 2012.

[5.] Murad A. Rassam, M.A. Maarof and Anazida Zainal" *A Survey of Intrusion Detection Schemes in Wireless Sensor Networks*", American Journal of Applied Sciences 9 (10): 1636-1652, 2012
ISSN 1546-9239 © 2012 Science Publication

[6.] Djallel Eddine Boubiche1 and Azeddine Bilami, "*Cross Layer Intrusion Detection System for Wireless Sensor Networks*," International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012

[7.] Pankaj Kumar Srivastava, Priyanka Rai, Upama Singh, " *Intrusion Detection: An Energy Efficient Approach in Heterogeneous WSN*", International Journal of Scientific and Research Publications, Volume 2, Issue 11, November 2012 1 ISSN 2250-3153.

[8.] Nabil Ali Alrajeh, S. Khan, and Bilal Shams," *Intrusion Detection Systems in Wireles Sensor Networks: A Review*" Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2013, Article ID 167575, 7 pages

[9.] Okoli Adaobi, Mona Ghassemian," *Analysis of an Anomaly-based Intrusion Detection System for Wireless Sensor Networks*" Ist International Conference on Communication engineering, University of Sislan and Baluchisthan

[10]. Jasvinder Singh, Er. Vivek Thapar," *Intrusion Detection System in Wireless Sensor Network*", International Journal of Computer Science and Communication EngineeringVolume 1 Issue 2 (December 2012 Issue)

[11.] Tapolina Bhattasali , Rituparna Chaki, "*A Survey of Recent Intrusion Detection Systems for Wireless Sensor Networks"* Techno India College of Technology,Kolkata,India

[12.] Ruchi Bhatnagar , Dr. A.K. Srivastava,Anupriya Sharma "*An Implementation Approach for Intrusion Detection System in Wireless sensor Network*" (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 07, 2010, 2453-2456