IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

Comparison of Various Intrusion Detection Systems in Wireless Sensor Network

Mohd. Abdul Sattar[1], Mohd. Anas Ali[2]

Associate Professor& Head, Dept of ECE, Nawab Shah Alam Khan College of Engineering & Technology, Hyderabad, India[1]

Low Voltage Electronics Security System Engineer, Techno I Electronics Security Systems, Hyderabad, India[2]

Abstract: Wireless Sensor Network is one of the most important part in the field of Communication Technology because it costs less installation charges and has simple network operation. In present days, WSN is used widely in each of the important sector which requires confidentiality and security, hence WSN requires very advance security system. Basically Wireless Sensor Network system suffers from two types of attacks one is active and another is passive. When confidentiality is the most important aspect of any secured network, then it is better to detect intruder before it really harms the network. Therefore for operating a WSN in secure manner, many intrusion detection systems (IDS) were proposed. In this paper we are conducting the comparative study on IDS for wireless sensor networks with their advantages and disadvantages. We are also describing the future research issues and challenges along with their complexity.

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

I. INTRODUCTION

Wireless sensor networks (WSN), sometimes called wireless sensor and actuator networks (WSAN), are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

The WSN is built of 'nodes' – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning 'motes' of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding. Deployment cost of Wireless Sensor Networks is low and it is easy to handle, so WSNs are applied over various fields of science and technology. WSN has wider range of applications; it is used for collecting much information regarding human activities and behaviour, like health care, military surveillance, highway traffic; it is also used to monitor physical and environmental phenomena, such as ocean and wildlife, earthquakes, pollution, wild fire, water quality etc. Another application of WSN is that it can be used to monitor industrial sites, such as building safety, manufacturing machinery performance, and so on. It is clear that Wireless Sensor Network (WSN) deals with many of the important information resources like military, health care, finance applications etc. Hence security of WSN is an important issue, especially if they have confidential information. For example in any condition command record of tactical (military) applications cannot be given to anybody. Failure in securing WSNs causes much harmful effect like, in a military operation, leak of command through security gap in the network would cause causalities of the friendly forces in a battlefield. Such type of security breaches that may humiliate the reliability and performance of the whole network easily wound wireless sensor networks (WSNs).

Wireless sensor network is vulnerable to several security threats. There are:

1. Misdirection: Changing or replaying the routing information can cause the misdirection attack. Forwarding the message along with the wrong path can cause this kind

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

of attack. Misdirection attack is also counted as routing layer attack.
2. Selective Forwarding: In this type of attack, attacker refuses to forward packets or drop them and acts as a black hole.
3. Sinkhole Attack: In Sinkhole attack, attackers attract all the traffic from a particular area to a compromise node. This kind of attack can also cause selective forwarding attack.
4. Sybil Attack: In Sybil attack, a malicious node can represent multiple identities to the network.
5. Wormhole Attack: The simplest form of this attack is an attacker sits in between the two nodes and forwards in between them.
6. Hello Flood Attack: In Hello Flood Attack, attacker broadcasts hello packets to the networks to add himself as the neighbour to the other nodes.

Sensor Network Layers and DoS Defenses		
Network Layer	Attacks	Defenses
Physical	Jamming	Spread-spectrum, priority messages, lower duty cycle, region mapping, mode change
	Tampering	Tamper-proofing, hiding
Link	Collision	Error-correcting code
	Exhaustion	Rate limitation
	Unfairness	Small frames
Network and Routing	Neglect and Greed	Redundancy, probing
	Homing	Encryption
	Misdirection	Egress filtering, authorization, monitoring
	Black Holes	Authorization, monitoring, redundancy
Transport	Flooding	Client Puzzle
	De-synchronization	Authentication

Fig. 1

II. INTRUSION DETECTION SYSTEMS

A computer system should provide assurance of confidentiality, integrity and fortification against intrusion. Since, due to increased connectivity on internet, and the evolution of vast spectrum of real time applications, e-commerce, e-business and more and more systems are subject to attack by intruders. Intrusion is defined as, process of intervening as burglar in between two authentic entities and the attempt to compromise the integrity, confidentiality or availability of a resource. And a system which is installed to take care of such ill activities by detecting them and keeps updated both entities is called Intrusion detection system.

Intrusion detection systems (IDS) can be classified into different ways. The major classifications are Active and passive IDS, Network Intrusion detection systems (NIDS) and host Intrusion detection systems (HIDS), Knowledge-based (Signature-based) IDS and behaviour-based (Anomaly-based) IDS

1. Active and passive IDS
An active Intrusion Detection Systems (IDS) is also known as Intrusion Detection and Prevention System (IDPS) which is configured to automatically block suspected attacks without any intervention required by an operator. It has the advantage of providing real-time corrective action in response to an attack. A passive Intrusion Detection Systems (IDS) is a system that is configured to only monitor and analyse network traffic activity and alert an operator to potential vulnerabilities and attacks. It is not capable of performing any protective or corrective functions on its own.

2. Network Intrusion detection systems (NIDS):
Network Intrusion Detection Systems (NIDS) 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.

3. Host Intrusion Detection Systems (HIDS):
HIDS is installed on workstations which are to be monitored. The agents monitor the operating system and write data to log files and/or trigger alarms. It can only monitor the individual workstations on which the agents are installed and it cannot monitor the entire network and is used to monitor any intrusion attempts on critical servers. The drawbacks of Host Intrusion Detection Systems (HIDS) are:

i) Difficult to analyse the intrusion attempts on multiple computers.
ii) Host Intrusion Detection Systems (HIDS) can be very difficult to maintain in large networks with different operating systems and configurations.
iii) Host Intrusion Detection Systems (HIDS) can be disabled by attackers after the system is compromised.

4. A knowledge-based (Signature-based) Intrusion Detection Systems (IDS): It references a database of previous attack signatures and known system vulnerabilities. The meaning of word signature, when we talk about Intrusion Detection Systems (IDS) is recorded evidence of an intrusion or attack. Each intrusion leaves a footprint behind (e.g., nature of data packets, failed attempt to run an application, failed logins, file and folder access etc.).

These footprints are called signatures and can be used to identify and prevent the same attacks in the future. Based on these signatures Knowledge-based (Signature-based) IDS identify intrusion attempts. The disadvantages of Signature-based Intrusion Detection Systems (IDS) are signature database must be continually updated and maintained and Signature-based Intrusion Detection Systems (IDS) may fail to identify unique attacks.

5 A Behaviour-based (Anomaly-based) Intrusion Detection Systems (IDS): It 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. Higher false alarms are often related with Behaviour-based Intrusion Detection Systems (IDS).

DOI 10.17148/IJARCCE.2016.51179

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

III. ADVANCED INTRUSION DETECTION SYSTEM

In this IDS, the combination of Energy Prediction based IDS, Hybrid Intrusion Detection System as well as the Cross Layer IDS are implemented. This is 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:

Si – 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 Si
If N(a)≠ ϕ
Select a
SN= j/the distance between a and N(a)< (rsi/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 evolution 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. That means the security attacks cause the sensor nodes to consume more energy.

So whichever node is consuming more power will be the affected one. In this way using the Energy Prediction System, 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 monitored 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. have a predefined energy consumption rate and that means if the present energy consumption rate matches with any of these the IDS, it clearly finds out the attack and gives a clear cut indication.

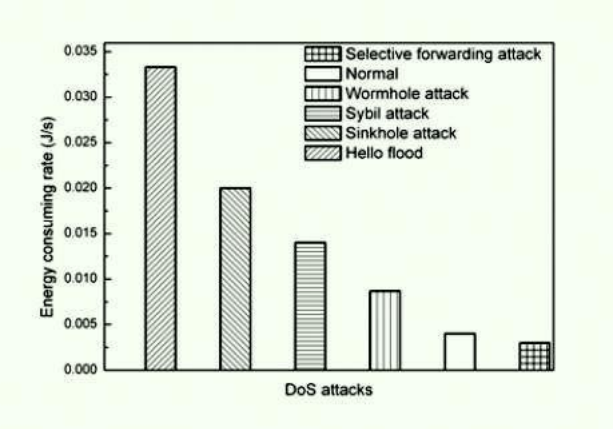

Fig-2

Fig- shows the graph in which the energy consumption rate vs denial of Service attacks is given. So from this the attacks energy consumption behavior can be clearly understood.

Problem arises when the energy consumption of the sensor nodes increases with the internal problems itself. 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 occurring between the OSI layers. Also a combination system which had Energy Prediction based as well as the Hybrid IDSs will work efficiently for small or medium sized wireless sensor networks.

For a large network with many number of sensors, it will not be suitable. So we can use the cross Layer IDS also along with it. Therefore 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.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

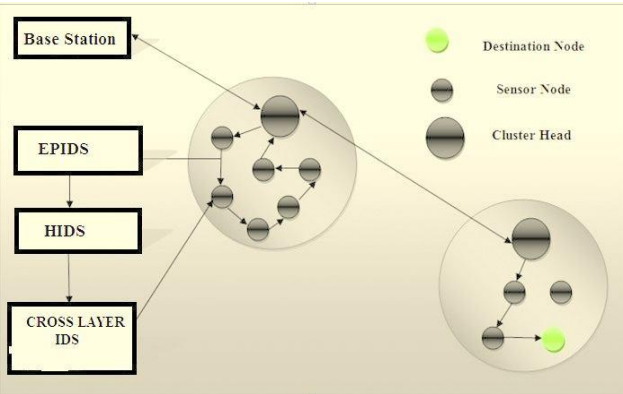

Fig-3

Fig. 3 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

According to Joseph Rish Simenthy, K. Vijayan, 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. The IDSs were performed in various levels. But in order to claim that the proposed IDS is perfect, there is a need to compare the performance of the current system with the existing ones. Fig- 4 clearly depicts the Delivery Ratio vs Percentage of affected nodes. In this case The Hybrid Intrusion Detection System as well as the Energy Prediction Based Intrusion Detection System were compared with the proposed Advanced Intrusion Detection System.

In the graph the red line represents the performance of the Hybrid Intrusion Detection System, the blue line represents the Energy Prediction based Intrusion Detection System and the green line represents the proposed Advanced Intrusion Detection System. It is clearly recognizable from the graph that the performance of the energy prediction system is very low when the percentage of the affected nodes increases.

That means, the delivery radio gradually 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 represents 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 From the performance graph we can conclude that the system gives better results than the Energy Prediction Based Intrusion Detection System and the Hybrid Intrusion Detection System. Thus when the percentage of affected nodes increases the Advanced Intrusion Detection System gives better results.

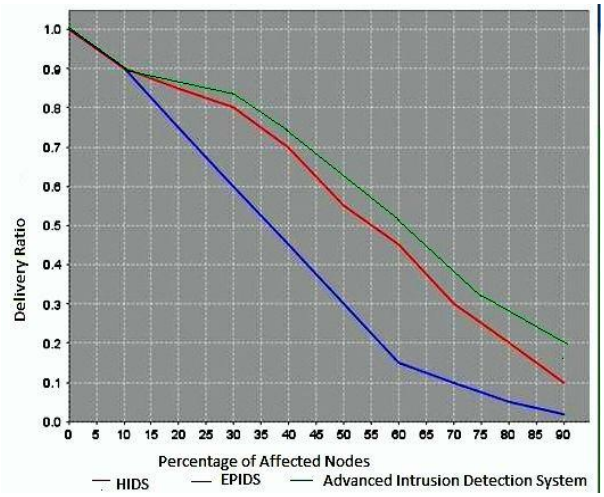

Fig-4

Joseph Rish Simenthy, K. Vijayan also 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 it was aimed to know the false positive probability too. A graph was plot in which Detection probability vs False Positive probability and the performance of the four IDS were compared.
This is shown in the Fig- 5. Here in the graph, the red line shows the Energy prediction Based Intrusion Detection System, the blue line shows the Hybrids 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 it can be analyzed 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 than 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.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

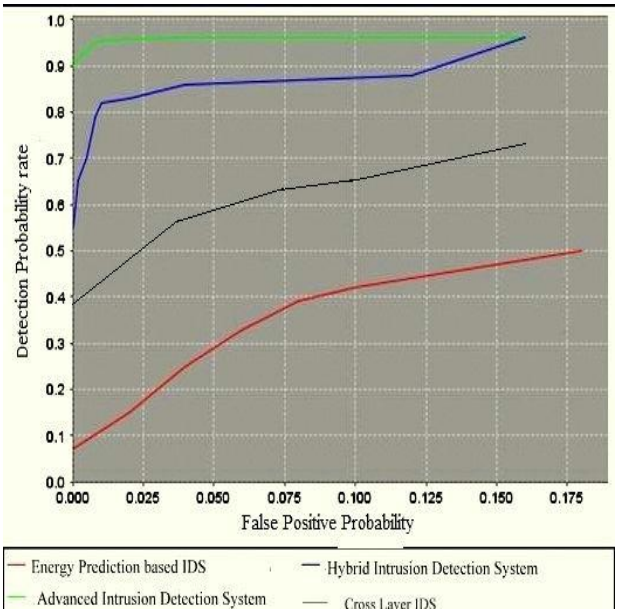

Fig-5

MAJOR ISSUES IN WSN

A. Security
Security in a sensor network is very challenging in WSN as it is not only being deployed in battlefield applications but also for surveillance and building monitoring applications.

B. Quality of service
The QoS in WSN is difficult because the network topology may change constantly.

C. Localization
The sensors are placed lacking their position in advance and once it is deployed there is no supporting infrastructure available to locate and manage them.

D. Deployment
Sensor nodes can be deployed either by placing one after another in sensor field or by dropping it from the plane. Sensor nodes are placed in real world, node death due to energy exhaustion either caused by normal battery discharge or due to short circuits is a common problem which may lead to wrong sensor readings.

E. Medium Access Control
Communication is a major source of energy consumption in WSN and MAC protocol directly control radio of nodes in network. MAC protocol should avoid collisions from interfering nodes.

DESIGN CHALLENGES OF WSN

A. Scalability
The network must preserve its stability. Introducing more nodes into the network means that additional communication messages will be exchanged, so that these nodes are combined into the existing network.

B. Fault tolerance and adaptability
Fault tolerance means to maintain sensor network functionalities without any interruption due to failure of sensor node because in sensor network every node have limited power of energy so the failure of single node doesn't affect the overall task of the sensor network.

C. Node Deployment
Sensor network can be deployed randomly in geographical area. After deployment, they can be maintained automatically without human presence.

D. Power Consumption
Wireless sensor node is microelectronic device; means it is equipped with a limited number of power sources. Nodes are dependent on battery for their power. Therefore power preservation and power management is an important issue in wireless sensor network.

E. Production Cost
As the name production cost suggests, we know that in the sensor network we have a large no of nodes deployed, so if the cost of a single node is very high then the cost of overall network will be very high.

F. Limited Computational Power and Memory Size
It is another factor that affects WSN in the sense that each node stores the data individually and sometimes more than one node stores same data and transfers to the base station which wastes the power and storing capacity of nodes, so we must develop effective routing schemes and protocols to minimize the redundancy in the network.

G. Security
Security is very important parameter in sensor network since sensor networks are data centric so there is no particular ID associated with sensor nodes and attacker can easily get inserted himself into the network and can steal the important data by becoming the part of network without the knowledge of sensor nodes of the network. So it is hard to identify whether the information is legal or not.

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, a Comparison of various Intrusion Detection System has been discussed and suggestions for improvements proposed.

As a result, it improves the detection rate and efficiency so that almost all the Intrusions can be detected. Also the discussed 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 can be greatly improved.

DOI 10.17148/IJARCCE.2016.51179

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

ACKNOWLEDGMENT

We express our sincere gratitude to **Prof. Mohd. Muzaffar Ahmad,** Electronics & Communication Engineering Department, Nawab Shah Alam Khan College of Engineering & Technology, Hyderabad, for extending his valuable insight.

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 Heterogeneous Wireless Sensor Networks", IEEE Transactions on Mobile Computing, Vol. 7, No. 6, June 2008, 698-711

[4.] 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, 2012ISSN 1546-9239 © 2012 Science Publication

[5.] 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

[6.] 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.

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

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

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

[10] 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

[11] Joseph Rish Simenthy, K. Vijayan "Advanced Intrusion Detection System for Wireless Sensor Network" (IJAREEIE) International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 3, Special Issue 3, April 2014 p. 167-172

BIOGRAPHIES

MOHD ABDUL SATTAR received B.Tech. Degree in Electronics and Communication Engineering from National Institute of Technology (NIT), Warangal and M.Tech. in Embedded Systems from JNTUH. He is an Associate Professor& Head of the Dept. of ECE in Nawab Shah Alam Khan College of Engineering & Technology, Malakpet, Hyderabad. He is also a member of IEEE.

MOHD ANAS ALI, received B.Tech. Degree in Electronics and Communication Engineering from Pujya Shri Madhavanji College of Engineering & Technology affiliated to JNTU Hyderabad in 2013 & M.Tech. degree in Embedded System from Nawab Shah Alam Khan College of Engineering & Technology. He is presently working at Techno I Security Systems, Abids, Hyderabad.