iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** IX **Month of publication:** September 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 4 Issue IX, September 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Review of Intrusion Detection Schemes in Wireless Sensor Network

Rakesh Sharma
Department of Computer Science, CRM Jat College, Hisar

Abstract: ***Wireless sensor networks area unit presently the greatest innovation within the field of telecommunications. WSNs have a wide range of prospective applications, including security and carry on watch over investigation, control, actuation and maintenance of complicated systems and fine-grain surveillance of indoor and outside environments. However security is one of the foremost aspects of Wireless sensor networks attributable to the resource limitations of detector nodes. Those networks are facing many threats that have an effect on their functioning and their life. In this paper we analysis the recent Intrusion Detection schemes in WSNs.***

KEYWORDS Wireless sensor Networks, Security, attack, Denial of Service (DoS), Intrusion Detection Systems (IDS), IDS Architectures, Cluster-based IDS, Anomaly-based IDS, Signature based IDS & Hybrid IDS

I. INTRODUCTION

Recent advances in wireless and micro electronic communications have enabled the development of a type innovative style of wireless network known as wireless sensing element network (WSN).Wireless sensor networks are associated with vulnerable characteristics like outdoor transmission and self-organizing while not a set infrastructure [1]. Consequently security of wireless sensor networks (WSN) is the most challenge for this kind of network [2]. Intrusion Detection Systems (IDSs) can play Associate in Nursing vital role in monitor investigation and preventing security attacks. This paper presents a review of the security attacks in wireless sensor network and analyzed a number of the prevailing IDS models and architectures.

Wireless sensor networks square measure not proof against the risks of destruction and decommissioning. Some of these risks are similar to those in Ad-Hoc networks, and others are specific to the sensors. Several articles [6][7][8][9][10] have given security attacks and problems in WSNs. Intrusion detection system (IDS) defined as the second line of defense when cryptography, allows the detection and bar of internal and external attacks.

In [18], it is presented a Rule-based ID known as conjointly Signature-based. Most of the techniques in these schemes follow three main sections: knowledge acquisition phase, rule application section and intrusion detection phase. In [19], it is proposed two approaches to boost the protection of clusters for sensing element networks victimization IDS. The first approach uses a model-based on authentication, and the second scheme is named Energy-Saving. In [21] a hybrid intrusion detection system (HIDS) model has been anticipated for wireless sensor networks. We will classify the safety goals into goals: main and secondary. The main goals include security objectives that ought to be offered in any system (confidentiality, availability, integrity and authentication). The other class includes secondary goals (self-organization, secure localization, Time synchronization and Resilience to attacks) [3] [4].

Confidentiality (Forbid access to unwanted third parties)
Authentication (Identity verification and validation)
Availability (Service has to be invariably available)
Integrity (Data is exchanged while not malicious alteration)
Self Organization(Every sensor node wants to be freelance and versatile enough to be self-organizing and self-healing)
ecure localization (Sensor network often wants location data accurately and automatically)
Time synchronization (Sensor radio may be turned off sporadically so as to conserve power)
Resilience to attacks (The covenant of a single node must not violate the safety of the complete network).

A. Security Attacks in WSN

The different characteristics of wireless device networks (energy restricted, low-power computing, use of radio waves, etc...) expose them to many security fears. We will classify the attacks into two key classes [5]: Active and Passive. In passive attacks, attackers are usually useable, i.e. hidden, and tap the communication lines to collect knowledge. In active attacks, malicious acts are carried out not solely against knowledge confidentiality however conjointly knowledge integrity. Several papers have bestowed the security

©IJRASET: All Rights are Reserved

attacks in WSN [6][7][8][9][10].

Spoofed, altered or replayed routing information

May be used for loop construction, attracting or repelling traffic, extend or shorten source route.

Selective forwarding In this attack, the attacker prevents the transmission of some packets. They will be removed later by the malicious node.

Worm hole attack:bThe wormhole attack needs insertion of at least 2 malicious nodes. These two nodes are interconnected by a powerful connection as an example a wired link. The malicious node receives packets in one section of the network and sends them to another section of the network.

Sybil attack: A malicious node presents multiple identities to the other nodes within the network. This poses a significant threat to routing protocols and can cause the saturation of the routing tables of the nodes with incorrect information. Black hole attack:The attack involves inserting a malicious node in the network. This node, by various suggests that, will modify the routing tables to force the maximum neighboring nodes passing the data through him. Then like a region in space, all the information which will come in it'll ne'er be retransmitted. Hello Flooding:

Discovery protocols on WSNs use HELLO messages varieties to discover its neighboring nodes. In an attack type hi Flooding, an assaulter can use this mechanism to saturate the network and consume energy.

Acknowledgement spoofing

In this attack, the attacker tries to win over the sender that the weak link is sturdy or that a dead node is alive. Therefore, all packets passing through this link or this node will be lost.

Denial-o Service Attacks A denial-of-service (DoS) targets the availability and capability reduction of network services. Physical constraints of the sensor networks and the nature of their preparation setting, make them vulnerable to DoS attacks over the other sort of network. In this section we are going to review important DoS eventualities for every layer of the WSN. In [11] Wang et al. (2006) have classified the DoS attacks that could target every layer of the WSN.

B. Countermeasures

To counter the attacks threatened networks wireless sensors, several analysis groups area unit making an attempt to search out applicable solutions. These solutions must take into account the specificities of wireless device networks. We want to search out easy solutions to secure the network whereas intense the smallest amount attainable energy and adapt these solutions to an occasional power computing. In the range of those solutions embrace mechanisms like knowledge partitioning, the use of appropriate cryptologic strategies, and intruder detection by location or even the arrogance index. Wood and Stankovic [12] studied DoS attacks and possible defense. In [13][14] a suite of optimized security protocols for wireless sensor network is conferred. SPIN (Security Protocol for Information via Negotiation) has 2 security mechanisms: SNEP and TESLA. SNEP provides knowledge confidentiality and data authentication. TESLA provides source authentication in multicast eventualities by mistreatment raincoat chaining. It is supported loose time synchronization between the sender and also the receivers. INSENS (Intrusion Tolerant routing for wireless sensor networks) this protocol permits the base station to draw Associate in nursing correct map of the network which will establish the routing tables for every node [15]. Du,et al. [16] propose LEAP+ (Localized Encryption and Authentication Protocol), a key management protocol for sensor networks.

II. INTRUSION DETECTION SYSTEMS IN WSN

After the construct of intrusion detection (ID), which was established in 1980, two major variants of intrusion detection systems (IDS) have emerged, Host intrusion detection systems (HIDS) and network intrusion detection systems (NIDS) [17]. Intrusion detection is an approach that is complementary with relation to thought of security mechanisms like cryptography and access management [18]. Intrusion detection are often outlined as Intrusion detection will be defined because the automatic detection and alarm generation to report that an intrusion has occurred or is ongoing. In this section we describe the design of IDS in WSNs. IDS cannot take preventive action, since they are passive in nature, they can solely discover intrusion and generate an alarm. The following figure presents the four main components of IDS [19].

There are two distinct technologies of IDS:

Network Intrusion Detection System (NIDS). These systems are designed to intercept and analyze packets current in the network. All communication in the wireless network are conducted on the air and a node will hear the traffic passing from a neighboring node

©IJRASET: All Rights are Reserved

(promiscuous mode) [36]. Therefore, the nodes can reciprocally check the network traffic. This technology applies this concept, IDS listens for traffic and individually examine every packet.

Host intrusion detection systems (HIDS). Analysis only knowledge on the node wherever the IDS is put in. Any decision is primarily based on data collected at this node. These IDSs use two sorts of sources to supply data regarding the activity: the log files (file that records all activity on a system in standby), and audit trails (Incoming / outgoing packets node, etc).

A. The difficult of planning IDS for WSN

The IDS solutions developed for wired networks cannot be applied on to sensor networks, view the distinction between these two sorts of networks, this is why it's necessary to introduce an intrusion detection system that meets the special options of detector networks [20]. The design of this sort of system for wireless detector network should satisfy the subsequent properties:

In wireless sensor networks, the IDS must satisfy the following properties [21]:

Localize auditing: IDS for wireless sensor networks should work with native knowledge and partial audits, because in WSN there square measure no centralized points (apart from the station base) which will collect international knowledge auditing.

Minimize resources: IDS must use a minimum range of resources for networks. Communication between nodes for intrusion detection should not saturate the obtainable information measure.

Trust no node: Unlike wired networks, nodes sensors can be compromised simply, IDS must not trust any node.

Be distributed: means that the gathering and analysis of information ought to be in many locations. Moreover the distributed approach conjointly applies to the execution of the algorithmic rule of detection and alert correlation.

Be secure: IDS must be in a position to stand up to attacks.

B. Architectures for IDS in Wireless Device Network

The nature of wireless sensor networks makes them terribly susceptible to attack. The Mobile nodes are willy-nilly distributed, there are no physical obstacles for the antagonist, therefore, they can be simply captured, and attacks can come back from all directions and target any node. To tackle these additional challenges, several doable IDS architectures exist as well as standalone IDS, distributed and cooperative IDS and hierarchical IDS [22].

1) Standalone IDS: In this category, each node operates as freelance IDS and is accountable for the detection of attacks against him. Therefore, the IDS don't cooperate and do not share info with one another. This architecture needs that every node is capable of death penalty and running IDS.

2) Distributed and Cooperative IDS: In this architecture (Zhang et al., 2003), each node has associate IDS agent and makes native detection choices by itself, all the nodes cooperate to produce a world detection method. The distributed and cooperative IDS architecture is a lot of appropriate for a flat network configuration than a cluster-based multilayered one.

3) Stratified IDS: In this category the network is split into clusters with cluster-heads. In each cluster, a leader plays the role of cluster-head. This node is responsible for routing within the cluster and should settle for messages from members of the cluster indicating one thing malicious. Similarly, the cluster-head must observe attacks against alternative cluster-heads in the network. At the same time all cluster-heads can work with central base station to create world IDS.

C. Some open analysis in IDS

Cross-Layer IDS: Using a cross layer IDS, we may not solely pass info between layers however additionally coordinate mechanisms to forestall threats in the least layers.

Dynamic IDS: The IDS that would protect mobile nodes, as in VANET networks.

Internet of Things IDS: There ought to be mechanisms that may manage all the objects of our existence that have associate information science address and be connected to the net.

III. INTRUSION DETECTION MODELS FOR WSN

Due to architectural distinction between wired and wireless networks, their IDSs cannot be used interchangeably. There are specific techniques for WSN [23]. In this section, we analyze and discus some planned IDSs for WSN.

A. Rule-based IDS

Rule-based IDS called additionally Signature-based IDS, articulates on a database of keep previous rules of security attacks [24].

©IJRASET: All Rights are Reserved

Most of the techniques in these schemes follow three main parts: knowledge acquisition phase, rule application part and intrusion detection phase (Silva et al., 2005) [25]. The algorithm includes 3 steps for detective work intrusions. In the opening monitor nodes monitors the info. In the second step detection rules are going to be ranked so as of severity, to the collected information to flag failure. The third step is the intrusion detection phase, where the variety of failure flagged is compared to the expected variety of the occasional failures within the network.

B. Cluster-Based IDS

Su, et al. [26] has proposed 2 approaches to improve the protection of clusters for detector networks victimization IDS. The first approach uses a model-based on authentication, which will resist to external attacks. Its basic technique is to add a message authentication code (MAC) for every message. Whenever a node wants to send a message, it adds to it a timestamp and a MAC is generated by a key-pair or separately counting on the key role of the sender (cluster-head, member -node, or base station). So that the receiver will verify the sender, the security mechanism is employed LEAP. The second scheme is known as Energy-Saving. This approach focuses on the detection of misbehavior each in Member nodes (MN) and cluster-head nodes (CH). When misconduct is detected, the CH broadcasts a warning message encrypted with the cluster key to restrain this specific node.

C. Hybrid IDS

In the Hybrid Approach, both techniques (Cluster-Based and Rule-Based) square measure combined to kind Hybrid detection technique. Hybrid detection exploits the advantages of each approaches provides simplicity, high safety, low consumption of energy [27] [28].The Hybrid Intrusion Detection System achieves the goals of high detection rate and low false positive rate.

III. CONCLUSION

This article shows how well a security detector networks may be a challenge for researchers and developers of knowledge technology. Our goal was to present the existing security attacks in WSN, focusing on intrusion detection systems (IDS), and examine existing approaches of intrusion detection in WSN. Our goal was to present the existing security mechanisms for WSN, specifically focusing on intrusion detection systems (IDS), and consider existing approaches to offer a reasonably comprehensive and effective model. We area unit currently operating on our own model that comes with all the benefits of the approaches planned for a worldwide model of intrusion detection in WSN

REFERENCES

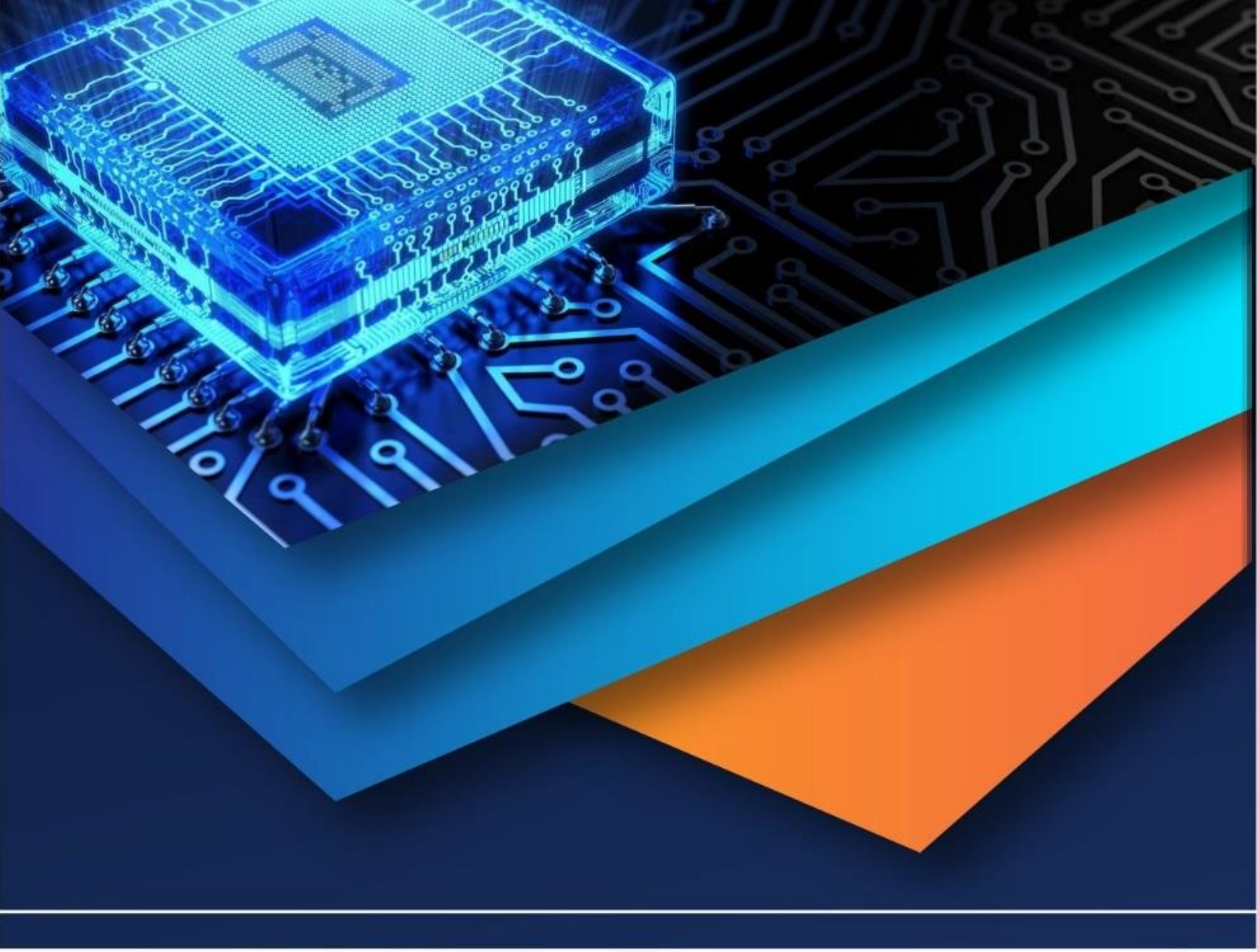
[1] Gang Zhao, “Wireless Sensor Networks for Industrial Process Monitoring and Control: A Survey”, Network Protocols and Algorithms, ISSN 1943-358, Vol. 3, No. 1, 2011.
[2] G. Padmavath, D. Shanmugapriya, “A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks”, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009.
[3] Qusay Idrees Sarhana, “Security Attacks and Countermeasures for Wireless Sensor Networks: Survey”, International Journal of Current Engineering and Technology ISSN 2277 – 4106, June 2013.
[4] Z. BENENSON, M. CHOLEWINSKI, C. FREILING, “Vulnerabilities and Attacks in Wireless Sensor Networks”, Laboratory for Dependable Distributed Systems, University of Mannheim, 68131 Mannheim, Germany, 2010
[5] E. Çayırcı and C. Rong , “Security in Wireless Ad Hoc and Sensor Networks”, ISBN: 978-0-470-02748-6, 2009.
[6] . Mohanty, S. Panigrahi, N. Sarma and S. Satapathy, “Security issues in wireless sensor network data gathering protocols: a survey”, Department of Computer Science and Engineering Tezpur University, Tezpur, India 2010.
[7] Q. Idrees Sarhan, “Security Attacks and Countermeasures for Wireless Sensor Networks: Survey”, International Journal of Current Engineering and Technology, 2013.
[8] A. Singla, R. Sachdeva, “Review on Security Issues and Attacks in Wireless Sensor Networks”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013.
[9] V. Soni1, P. Modi, V. Chaudhri, “Detecting Sinkhole Attack in Wireless Sensor Network”, International Journal of Application or Innovation in Engineering & Management, Volume 2, Issue 2, February 2013.
[10] K. Sharma, M. Ghose, “Wireless Sensor Networks: An Overview on its Security Threats”, IJCA Special Issue on “Mobile Ad-hoc Networks” MANETs, 2010.
[11] K. Sun, P. Peng, P. Ning, and C. Wang, “Secure Distributed Cluster Formation in Wireless Sensor Networks”, in Proceedings of the 22nd Annual Computer Security Applications Conference (AC-SAC’06), Pages: 131-140, December 2006.
[12] Wood and J. Stankovic, “Denial of service in sensor networks”, IEEE Computer, pages 5462, October 2002.
[13] Ullah, Fasee, “Analysis of security protocols for Wireless Sensor Networks”, Dept. of Comput. Sci., City Univ. of Sci. & Inf. Technol., Peshawar, Pakistan, Computer Research and Development (ICCRD), 2011.
[14] A. Perrig, R. Szewczyk, J.D Tygar, V. Wen abd D. Culler, “SPINS:Security Protocols f or Sensor Networks”, Departement of electrical engineering and Computer Scinces, University of California, Berkley, USA 2002.
[15] J. Deng, R. Han, S. Mishra, “INSENS: Intrusion-Tolerant Routing in Wireless Sensor Networks”, University of Colorado, Department of Computer Science,

©IJRASET: All Rights are Reserved

Volume 4 Issue IX, September 2016
ISSN: 2321-9653

2002. \
[16] S. Zhu, S. Setia, and S. Jajodia, “LEAP & plus; Efficient security mechanisms for large-scale distributed sensor networks”, ACM Transactions on Sensor Networks (TOSN), Volume 2, Issue 4**,** November 2006.
[17] . Saha, Md. Safiqul Islam, Md. Sakhawat Hossen, “A New OHD Based Intrusion Detection System for Wireless Sensor Network”, IK2206: Internet security and privacy, 2010.
[18] F. Amini, “Simulation and Evaluation of Security and Intrusion detection in IEEE 802.15.4 Network”, university of Manitob 2008.
[19] Nabil Ali Alrajeh, S. Khan, and Bilal Shams, “Intrusion Detection Systems in Wireless Sensor Networks: A Review”, International Journal of Distributed Sensor Networks, Volume 2013. [20] Hassen Mohammed Abduallah Alsafi, 2 Saeed Salem Basamh, “A Review of Intrusion Detection System Schemes in Wireless Sensor Network”, Journal of Emerging Trends in Computing and Information Sciences, 2013.
[20] 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.
[21] Andreas A. Strikos, “A full approach for Intrusion Detection in Wireless Sensor Networks”, School of Information and Communication Technology , Stockholm, Sweden ,March 1, 2007.
[22] R. Roman, J. Zhou, J. Lopez, “Applying Intrusion Detection Systems to Wireless Sensor Networks”, Proceeding of the 3rd IEEE Consumer Communications and Networking Conference, 2006.
[23] Roosta, Tanya, Sameer Pai, Phoebus Chen, Shankar Sastry, and Stephen Wicker. "Inherent security of routing protocols in ad-hoc and sensor networks." In Global Telecommunications Conference, 2007. GLOBECOM'07. IEEE, pp. 1273-1278. IEEE, 2007.
[24] A. da Silva, M. Martins, B. Rocha, A. Loureiro, L. Ruiz, and H. Wong, “Decentralized intrusion detection in wireless sensor networks”, international workshop on Quality of service & security in wireless and mobile networks, 2005.
[25] C.-C. Su, K.-M. Chang, Y.-H. Kuo, and M.- F. Horng, “The new intrusion prevention and detection approaches for clustering-based sensor networks”, in 2005 IEEE Wireless Communications and Networking Conference, WCNC 2005: Broadband Wirelss for the Masses - Ready for Take-off, 2005.
[26] A. Abduvaliyev, A.K Pathan, J. Zhou, R. Roman and W. Wong, “On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks”, Communications Surveys & Tutorials, IEEE Volume 15 , Issue 3, 2013.
[27] Mr. Ansar I SheikhMr. Pankaj Kewadkar, “Approach towards Intrusion Detection System for Wireless Sensor Network”, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, 2013.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)