iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** VI **Month of publication:** June 2020

DOI: http://doi.org/10.22214/ijraset.2020.6231

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VI June 2020- Available at www.ijraset.com

Survey on Intrusion Detection System for various Attacks in IOT

Samiksha Khule[1], Abhilash Sonker[2]
[1]*Master of Technology,* [2]*Assistant Professor, Department of CSE & IT, Madhav Institute of Technology & Science, Gwalior-474001, India*
samiksha.khule94@gmail.com[1] *, abhilashsonkerit@gmail.com*[2]

Abstract: ***The conceptualize idea of internet of thing (IOT) is in trend now a days in which many devices are connected through internet in wireless manner. Constantly majority of devices were connecting together to the internet rather than the human intervention. As the devices in the IOT is resource constraint, so to serve the security in these devices is one of the considerable research issues, which leads the attack occurs in the whole network. The network layer Routing Protocol for Low Power and Lossy Networks (RPL) is the routing protocol suspectable for various security attacks. RPL is a light-weight protocol and it has no functionality like other traditional routing protocols have. Therefore, the Intrusion Detection System (IDS) is required. In this article we will spot to explore diverse security attacks as well as various IDS approaches to diminish those attacks.***
Keywords: Internet of Thing, RPL, Intrusion Detection System, Security, WSN

I. INTRODUCTION

IOT is considered as the fastest growing topic and the smart network which connects various objects in wireless medium in order to reach a common goal. The highest amount of the devices used in IOT are heterogeneous and resource constraint in terms of memory size and battery power. IOT allude to the physical objects which has the ability of exchanging information with other objects and various virtual components [1]. The aim of IOT is to enlarge the internet connectivity from standard devices like camera, vehicles etc. IOT contains numerous applications like smart-cities, smart-homes, smart-water, smart-environment and health monitoring [2].
There are numerous issues in the IoT network regarding the security of the devices and also there are issues regarding the evolution of various applications in IOT. If the problem of security must not be addressed on time then the essential information may be leaked anytime. Thus, the addressed security issues must be:

1) *Confidentiality:* The attacker can easily seize the passing of messages between source to destination. So that the content can be modified and privacy can be leaked. So, in IOT the secure message transferring is required.
2) *Integrity:* It means that the transmitted message should be valid from sender node. It guarantees the message that it should not be altered while transmission.
3) *Availability:* Resource or data must be available when required. To damage the availability the attacker can flow the bandwidth of resources. Some malicious attackers like denial-of-services (DOS) attack, flooding attack may harm the availability of various resources.
4) *Authenticity:* Authenticity assures the proof of identity. It concerns with truthfulness of correct users. So that fake user can not send data.
5) *Non- repudiation:* It confirms that sender and receiver cannot refuse having sending and receiving message respectively.
6) *Data Freshness:* It intend that whenever it is required the data must be recent. It assures that no attacker replayed old message.
7) *Storage:* This intended that the storage required sufficient to use. There should be no storage issues.
8) *User Privacy:* The data or resources used must have privacy no unauthorized user can access it. The security level is used to protect the private data, communication and preferences.

II. IOT PROTOCOLS

The protocols which are affected mostly are the Routing Protocol for Low-Power and Lossy-Network (RPL) and IPv6 over Low Power and Wireless Private Area Network (6LoWPAN).

A. RPL

RPL is a distance-vector protocol which supports various types of data-link protocols [3]. According to its name this protocol was especially designed for low-power and lossy-network, using IPv6 Border Router sink/root node in RPL is connected through internet directly.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VI June 2020- Available at www.ijraset.com

The nodes of RPL are power constraint, each and every node contains its own rank-id which assures its actual position within the network and also the nodes parents and nodes children. RPL has bidirectional communication as it is created on directed-tree graphs. In the form of Destination Oriented Directed Acyclic Graphs (DODAG) RPL creates routing topology.
RPL quickly creates new network routes, shares routing information in efficient way. Various attacks which occurred in the RPL network they were, like sinkhole attack, DODAG-Version attack, DIO suppression attack.

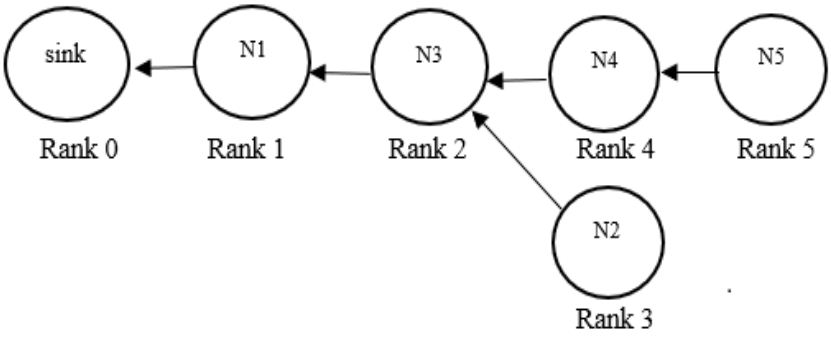


Fig.1. RPL Topology

B. 6LoWPAN

6LoWPAN is a lightweight standardized protocol is used for connecting various IoT devices. 6LoWPAN measures allow the effective use of IPv6 over low rate, low power wireless network through adaptation layer and related protocols on simple embedded device. This protocol is precisely designed for the resource-constrained devices in the IoT network [4]. The construction of 6LoWPAN-protocol is done with the help of the compression of the IPv6-protocol for the network layer. The 6BR (6LoWPAN Border Router) is the medium by which 6LoWPAN networks are connected to the internet. The compression, fragmentation and decompression of IPv6 datagrams is performed by 6BR.

III. IOT ARCHITECTURE

In IoT system architecture there are three layers as shown in Figure,.2:

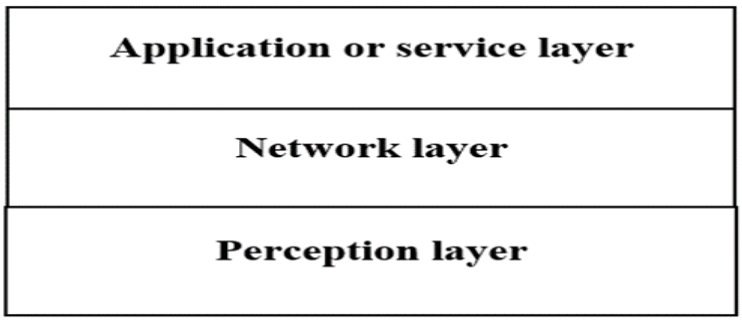


Fig.2. Internet of Thing Architecture

A. The Perception-Layer

The perception-layer is the primary layer which collects and observe each and every type of information used is IoT environment. This information is collected by using various type of sensors like: sound sensor, RFID sensor, GPS etc. [5].
The perception layer has two parts:

1) Perception node used to control data.
2) Perception network used to send data to controller.

B. The Network-Layer

The network layer is also termed as Transportation-layer because it has the transportation ability to send data from lower to upper layer [5]. The data or information is transmitted by this layer via internet. Therefore, the network layer joins various heterogeneous networks [17].

C. The Application-Layer

This application-layer is also known as Service layer. This layer is used to convert information into data or content and this layer also provides good user-interface (UI) to end user. This layer shares information in secure manner so no unauthorized user can read it [5].

IV. INTRUSION DETECTION SYSTEM

The illegal action which is done by attacker to breakdown network or destroy the sensor-nodes completely is termed as intrusion. Therefore, to monitor this type of intrusions the Intrusion Detection System (IDS) is used [6]. In particular nodes and network the Intrusion Detection System monitors the malicious traffic and unauthorized activities. The main objective of IDS is to detect the nodes and networks, inspect numerous intrusions in networks or nodes, and after the intrusion is detected it alerts the user. It avoids system damage by generating alert before it is begin attacked by attacker as it is works as an alarm or the network onlooker. Both external and internal attacks are detected by Intrusion Detection System. The network packets are detected by IDS to determine the intruders or legitimate users.

The Intrusion Detection System has mainly three components:

1) Monitoring components used to monitor local events as well as the neighbor events. As name suggested it monitors events, traffic patterns and resources in the whole network.

2) Analysis and detection based on modelling algorithm which is the main element of the IDS. In this process the network activity is analyzed and after that the decisions are made to announce them legal or illegal.

3) Alarm used to boost alarm. This element generates response as alarm just in case of intrusion detection [7] in the network.

A. Types of IDS

1) *Signature based Intrusion Detection Systems:* Signature based IDS is also known as Rule-Based IDS. This technique is easy to use static approach. There are various predefined rules of different security attack are stored in signature-based IDS. It matches the existing patterns of a network from pre-defined attacks patterns or signature. For known intrusion the Signature based IDSs are well suited. Therefore, the specific knowledge of single attack is needed. Signature based IDS are host-based IDS in which each node has IDS system. This is very expensive approach as it needs more storage. Signature based IDS technique cannot analyse new attacks unless their patterns or signature are added manually in the database. That's why the database of this technique needs regular upgradation of new patterns or signature of attacks [8].

2) *Anomaly based Intrusion Detection Systems:* Anomaly based IDS is also known as Event-Based IDS. Using heuristic approach this technique observes the networks normal or malicious activities. The intrusion in anomaly-based IDS technique is detected using threshold value [9]. Therefore, the resultant value below the threshold value is normal whereas the condition above the threshold value is known as intrusion. The ability of detecting new and unknown attack is an advantage of this technique. Rather than the signature-based IDS the anomaly-based IDS detect the attacks in more efficient manner. This technique learns normal traffic pattern to detect the presence and absence of any type of intrusion.

V. CYBER ATTACKS ON IOT

The IoT network are disclosed of various classification of attacks, from the both internal as well as the external. There are basically two categories of attacks the first is inside attack, in which attack can be carried out by compromised or malicious node inside the network and second is outside attack, in which attacker is not the part of the network. Let's discuss some cyber-attacks:

1) *Wormhole Attack:* In wormhole-attack the attacker-node can easily launched the attack without having the knowledge of its entire network. The attacker-node creates a basic virtual-tunnel between two end users. Between the two actual nodes an attacker node acts as a forwarding node and the malicious node claims that they are one hope afar from the base station [10]. This attack keeps the attacker nodes at strong position as compared to the other nodes. The capturing of packet from one location to the other isolated location via virtual tunnel is done by the attacking nodes [11].

2) *Sinkhole Attack:* In the sinkhole-attack the attacker node promotes its fake routing update and tries to attack the network traffic. By creating the false node, the attack can be created inside the network [10]. The attacker node in this attack attracts the network traffic towards itself. By exhibits its routing-cost minimal the attacker nodes attract every adjacent node to forward their packets. To launch other type of attacks the sinkhole attack is used.

3) *Sybil Attack:* In this type of attack the attacker node has various multiple identities by stealing the identity of other legitimate nodes [10]. That's why the base station cannot differentiate the appropriate node and the attacker nodes. So, the performance of the network slows down due to this confusion. In the sybil attack the alike frequency is being shared between every node because of the broadcast and open communication medium in the network.

4) *Selective-Forwarding Attack:* In this type of attack the attacker node acts as a legitimate node but it selectively refuses to forward certain messages or selectively drop some packets assuring that they are not propagate further [10]. The easiest form of selective-forwarding attack is Blackhole Attack in which the attacker/malicious node drops all the packets in the network.
5) *Hello-Flood Attack:* In this network layer attack the Hello-message is broadcast by the routing-protocol to declare its existence to their neighbor. The legitimate node that receives Hello-message assumes that the sink-node is inside its normal radio range and it add that node as its neighbor-list [11]. Sometimes this assumption may be false therefore the network remains in the confusion state.
6) *Denial-of-Service (DOS) Attack:* In this type of attack the availability of the resources may damage. The resources have been made unavailable to its intended users when the Denial of Service attack is made. When various malicious node launched this attack, it is known as DDoS. The network resources, CPU time, bandwidth etc. may affect due to this attack.
7) *Man-in-the-Middle Attack:* In this attack the attacker possibly alters the communication between two the two legitimate nodes and makes them believe that they are communicating directly to each other without any interruption. This attack exploits real time processing of various transactions.

VI. LITERATURE REVIEW

The Internet of Thing has been popular from a long time. But the security in IoT network is the main issue. Even though the RPL protocol offers some set of mechanism against malicious activity for secure communication in the network. Following authors discussed some techniques used for detection of various attacks:

Shahid Raza [12] proposed a real-time intrusion-detection-system in IoT known as SVELTE. The only Intrusion-detection-system available in the IoT is termed as SVELTE which implements on Contiki-OS. In this paper there were mainly three centralized components placed in 6LoWPAN Border-Router. Very first component is 6LoWPAN, which collects all essential data regarding RPL-protocol and fix the network in 6BR. Intrusion detection component is the second element that analyze the mapped-data and also detects the presence of intrusion from that data. The third component is mini distributed firewall, which is used to filter malicious-traffic, before the traffic reaches to that network. Only the spoofing attack, selective forwarding and sinkhole attack is detected through this approach.

P. Pongle et al. [13] proposed the detection method of wormhole attack by novel IDS method in IoT which is implemented with the help of Cooja simulator in the Contiki OS. In this article the proposed-system uses distributed and centralized architecture for IDS placement. By using local information, the particular approach detects the various wormhole attack whereas with the use of neighbor information the attacker node is identified. As the result the true positive rate for wormhole detection id 94% and for the detection of both attack and attacker in 87%.

Yousef EL Mourabit [14] proposed an intrusion detection system in WSN based on mobile agent. The approaches in this paper make use of classification-based approach and multiple agent for intrusion detection. Three agents are used to detect intrusion. The collector is the first agent which is used to collect the required data from wireless network environment and carryforward the data. The second is misuse detection agent, with the help of various detection techniques it detects the known attacks. The anomaly detection agent is the third agent which leads to detects various unknown attacks by SVM classification algorithm with classification rate 97.4%. To detect the attack in future few parameters are proposed by creating complex detection parameters, using various statistical anomaly detection and able to create attack signature.

Khraisat et al. [15] proposed the detailed survey of methodology of intrusion detection system, types of intrusion detection system and technologies with their limitations and technologies. In this paper various machine learning techniques are proposed to detect zero-day attack. Also, the summarized result of recent research papers to the explored the contemporary model of improved performance of AIDS is discussed as the solution to overcome issues of IDS.

Ms. T. Eswari [16] proposed a framework of rule-based intrusion-detection-system for wireless sensor network. In this approach there were mainly three phases. The first phase mentions the phase of local auditing which checks the validation of packets to checks that the packets are arriving from the valid node or not. The rule application phase is the second phase, this phase works in promiscuous mode. The last third phase is the intrusion detection phase which is used to detect various routing attack by collecting valid data from content suppression unit. Only to detect routing attacks this security mechanism is used.

Kasinathan [18] proposed DoS detection architecture based on ebbits network framework for detection of various DoS attacks. In this approach by using IDS probe the 6LoWPAN traffic is monitored. For the placement of intrusion detection system, the hybrid approach is used. In this approach the DoS protection is the basic component which raise an alert on network manager component by using available information.

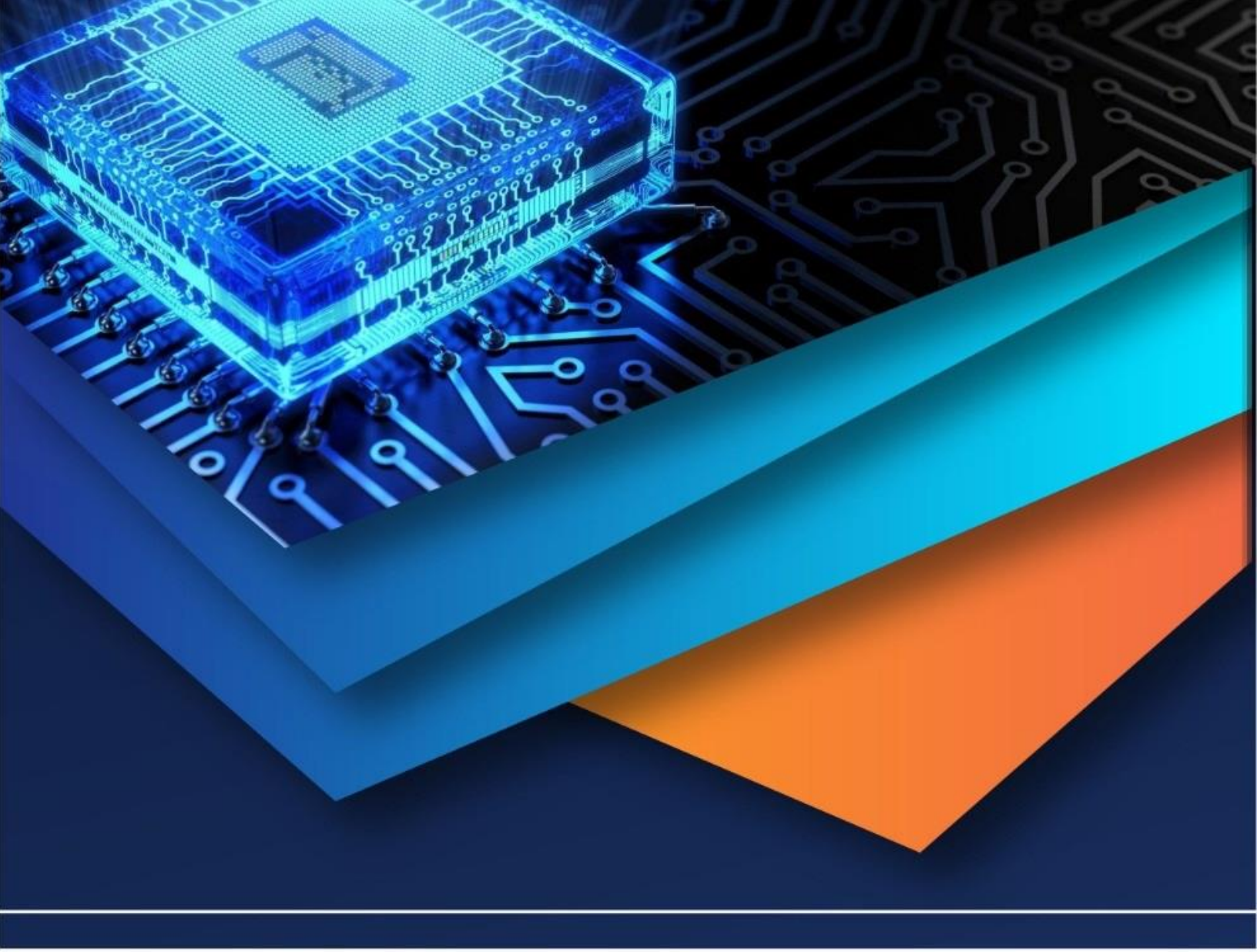
Samir Athmani [19] proposed an efficient Intrusion Detection System to detect blackhole attack in WSN is implemented NS2 network simulator. In this approach the control packets are exchanged between the base station and the sensor nodes. Each packet has its node id and also contains the number of packets which is sent to the cluster-head. The base-station detects the blackhole attack. This process uses less energy but has no guarantee that all blackhole attacks can be detected by this proposed approach but it can reduce some impacts of blackhole attacks.

VII. CONCLUSION

As the trend of IoT is increasing day by day, therefore the services, users and the applications of IoT is increases. So, for the ease use of IoT environment its necessary to have light weighted security solutions as the security issues cannot be ignored. In this survey, several papers were studied, these papers have the study of design and implementation of various approaches of intrusion detection system used in IoT network. Also, we discuss various security attacks made on IoT applications. The features of all IDS methods re summarized, we observe that the researches of IDS for various attacks in IoT is still growing, very few of them were precisely for IoT paradigm. So, we conclude that to design such system for detection and identification of various attacks and attackers were required for resources constrained sensor nodes of IoT.

REFERENCES

[1] Shanzhi Chen, Hui Xu, Dake Liu, Bo Hu, Hucheng Wang," A Vision of IoT: Application, Challenges, and Opportunities with China Perspective", IEEE Internet of Things Journal, Vol. 1, No. 4, August 2014.
[2] P. Gokul Sai Sreeram, Chandra Mohan Reddy Sivappagari," Development of Industrial Intrusion Detection and Monitoring Using Internet of Thing", International Journal of Technical Research and Applications, 2015
[3] T. Winter, P. Thubert, A. Brandt et al., "RPL: IPv6 routing protocol for low-power and lossy networks," RFC 6550, March 2012.
[4] T. Kushalnagar, G. Montenegro, C. Schumacher, IPv6 over Low-power Wireless Personal Area Network (6LoWPANs): Overview, Assumptions, Problem State- ment, and Goals, RFC 4919 (2007).
[5] Xiaolin Jia, Quanyuan Feng, Taihua Fan, Quanshui Lei, "RFID technology and its application in Internet of Things (IoT)", 2nd International Conference Electronics, Communications and Networks (CECNet), IEEE DOI: 10.1109/CECNet.2012.620150 8, 2012.
[6] A. Anand, B. Patel, "An Overview on Intrusion Detection System and Types od Attacks It Can Detect Considering Different Protocol", International journal of Advanced Re- search in Computer Science and Software Engineering, vol.2, no. 8, 2012
[7] S. Khan, K.K.Loo, and Z.U.Din," Framework for intrusion detection in IEEE 802.11 wireless mesh networks," International Arab Journal of Information Technology,vol.7,no.4,pp.435-440,2010.
[8] Neha Maharaj, Pooja Khanna," A Comparative Analysis of Different Classification Techniques for Intrusion Detection System", International Journal of Computer Application, 2014.
[9] V.Jyothsna,V.V.Rama Prasad," A Review of Anomaly based Intrusion Detection System",International Journal of Computer Application,2011.
[10] Okan CAN, Ozgur Koray SAHINGOZ," A Survey of Intrusion Detection System in Wireless Sensor Networks", 6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO), 2015.
[11] Abdur Rahaman Sardar, Rashmi Ranjan Sahoo, Moutushi Singh, Souvik Sarkar, Jamuna Kanta Singh, and Koushik Ma- jumder," Intelligent Intrusion Detection System in Wireless Sensor Network", Proc. Of the 3rd Int. Conf. on Front. Of Intell. Comput. (FICTA), 2014 Vol. 2, Advances in Intelligent Systems and Computing 328, Springer DOI: 10.1007/978-3- 319-12012-6 78.
[12] Shahid Raza and Linus Wallgrena, Thiemo Voigt," SVELTE: Real-time Intrusion Detection in the Internet of Thing," Ad Hoc Network (Elsevier), Vol. 11, No. 8, pp. 2661-2674, 2013.
[13] P.Pongle,G.Chavan,"Real Time Intrusion and Wormhole Attack Detection in Internet of Things",International Journal of Computer Applications (0975 - 8887),July 2015.
[14] Yousef EL Mourabit, Ahmed Toumanari, Anouar Bouirden, Hicham zougagh, Rachid Latif, "Intrusion Detection System In Wireless Sensor Network Based on Mobile Agent", Second World Conference on Complex Systems (WCCS), IEEE DOI: 10.1109/ICoCS.2014.7060910,2014.
[15] Ansam Khraisat, Iqbal Gondal, Peter Vamplew and Joarder Kamruzzaman," Survey of Intrusion Detection System: techniques, dataset and challenges", Springer Open 2019. https://doi.org/10.1186/s42400-019-0038-7.
[16] Ms. T. Eswari, Dr. V. Vanitha, "A novel Rule Based Intrusion Detection Framework for Wireless Sensor Networks", International Conference on Information Communication and Embedded System (ICICES), IEEE DOI: 10.1109/ICI-CES.2013.6508172,2013.
[17] Qi Jing, Athanasios V, Vasilakos, Jiafu Wan, Jingwei Lu, Dechao Qiu, "Security of the Internet of Things: perspectives and challenges", Published in Springers journal of Mobile Communication, Computation and Information, November 2014, Volume 20, Issue 8, pp2481-2501.
[18] Kasinathan,Prabhakar,et al."Denial-of-Service detection in 6LoWPAN based internet of things." Wireless and Mobile Computing,Networking and Communications (WiMob),2013 IEEE 9th International Conference on.IEEE,2013.
[19] Samir Athmani, Djallel Eddine Boubiche and Azeddine Bilami, "Hierarchical Energy Efficient Intrusion Detection System for Black Hole Attacks in WSNs", Published in Computer and Information Technology (WCCIT), 2013.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY