iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VIII **Month of publication:** August 2022

DOI: https://doi.org/10.22214/ijraset.2022.46036

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: 7.538
Volume 10 Issue VIII August 2022- Available at www.ijraset.com

Integration of Wireless Sensor Networks in Environmental Monitoring Cyber Infrastructure

Mrs. C. Nithya Praba[1], Dr. D.Kalaivani
[1]*Research Scholar (FT),* [2]*Associate Professor & Head, Department of Computer Science, Dr. SNS Rajalakshmi College of Arts and Science, Coimbatore-49.*

Abstract: ***Wireless sensor networks (WSNs) have great potential to revolutionize many science and engineering domains. We present a novel environmental monitoring system with a focus on overall system architecture for seamless integration of wired and wireless sensors for long-term, remote, and near-real-time monitoring. We also present a unified framework for sensor data collection, management, visualization, dissemination, and exchange, conforming to the new Sensor Web Enablement standard. Some initial field testing results are also presented. The monitoring system is being integrated into the Texas Environmental Observatory infrastructure for long-term operation. As part of the integrated system, a new WSN-based soil moisture monitoring system is developed and deployed to support hydrologic monitoring and modeling research. This work represents a significant contribution to the empirical study of the emerging WSN technology. We address many practical issues in real-world application scenarios that are often neglected in the existing WSN research.***
Keywords: Data collection, framework, hydrologic, sensor web.

I. INTRODUCTION

Due to recent advances in electronic industry, wireless sensors can be used in various ubiqutous and pervasive applications such as military, security, health-care[1, 2], industry automation, environmental and habitat monitoring [3, 4]. Wireless sensor networks (WSNs) consist of large number of low power nodes, with limited processing, communication, and storage resources [5]. Due to limited resources of WSNs, it is challenging to incorporate basic security functions, such as authentication, access control, data integrity, privacy, and key distribution. For instance, asymmetric cryptography such as RSA or Elliptic Curve cryptography (ECC) is unsuitable for most sensor architectures 2 Firdous Kausar, Ashraf Masood, and Sajid Hussain due to high energy consumption and increased code storage requirements. To avoid the use of asymmetric cryptography, several alternative approaches have been developed to perform key management on resource-constrained sensor networks, such as random key pre-distribution schemes, plain text key exchange schemes, and transitory master key schemes. In WSNs, hierarchical clustering provides scalability, self-organization, and energy efficient data dissemination [6]. A number of cluster formation protocols have been proposed but most existing protocols assume benign environments, and are vulnerable to attacks from malicious nodes. In this chapter, we use an existing ring structure energy efficient clustering architecture (RECA) [7] to divide nodes into clusters. However, we modify its initial cluster formation algorithm by providing an authentication mechanism, so that no malicious node can take part into cluster formation process. The proposed authenticated key management (AKM) scheme enables only legitimate nodes to join the network. The rest of the chapter is organized as follows: Section 2 discusses key distribution schemes, which are relevant to the proposed scheme. In Section 3, the AKM scheme is described in detail, such as nodes authentication prior to join a network, secure cluster-formation along with details about shared key discovery, and new node addition. Section 4 focuses on the performance and security analysis of the AKM scheme. Section 5 summarizes the major contributions of this work

Wireless sensor technology is playing a vital role in many of the commercialized industrial automation processes and various other real life applications [1–4]. It is particularly suitable for harsh environment applications where deploying of other network infrastructure is difficult and/or almost impossible such as in battlefield, in hazardous chemical plant, and in high thermal environment. It is not uncommon to see that most of the crucial surveillance and security applications also rely on sensor based applications. Sensors which are tiny in size and cheap in cost have the capabilities to be deployed in a range of applications as explained in [5–9]. Essentially all sensor networks comprise some forms of sensing mechanism to collect data from an intended physical environment either by a time driven approach or by event triggering approach.

By these approaches a sensor will convey the sensed data to a destination or sink (multiple destinations/sinks are also possible) via some kinds of routing algorithm such as Minimum Cost Forwarding Algorithm (MCFA), Directed Diffusion Routing Protocol (DDRP), or one of the cluster-based routing protocols. Being very small in size, sensor nodes are built with limited computational capacity, small storage memory, and finite battery power capacity [10].

The structure of a typical WSN node [11] consists of four main components: a sensing element, normally used for sensing a physically measureable parameter; an Analog-to-Digital Converter (ADC), used for converting analog signals to some digital formats; a processing unit, providing simple/basic data processing and computation capabilities; and a power unit, responsible for sensor node's operation life span. It is a known fact that WSN is a resource constrained network in which energy efficiency is always the main issue since the operation of WSN depends heavily on the life span of the sensor node battery [12]. The most energy consuming operation in WSN is the data packet routing activity. The characteristics of the WSN are different from the conventional networks [13, 14]. These unique characteristics are often taken into account for addressing the issues and challenges related to network coverage, runtime topologies management, node distribution, node administration, node mobility energy efficiency/consumption, network deployment, application areas/environment, and so forth [15–17].

Nodes in a WSN are generally energy, computation, and memory constrained. Consequently, there is a need for research and development into low-computation resource-aware algorithms for WSNs, targeting at small, highly resource constrained embedded sensor nodes. Energy consumption is of prime importance in WSNs and thus some algorithms [18–24] and hardware were designed with energy efficiency or energy awareness as a central focal point of interest. Enhancing energy efficiency of WSN with respect to the communication routing protocol is the primary concern of this research. We propose a new routing protocol entitled "Position Responsive Routing Protocol (PRRP)" and compare its performance with the well-known LEACH and CELRP protocols. The simulation results show a significant improvement over the aforementioned protocols in terms of energy efficiency and the overall performance of the WSN.

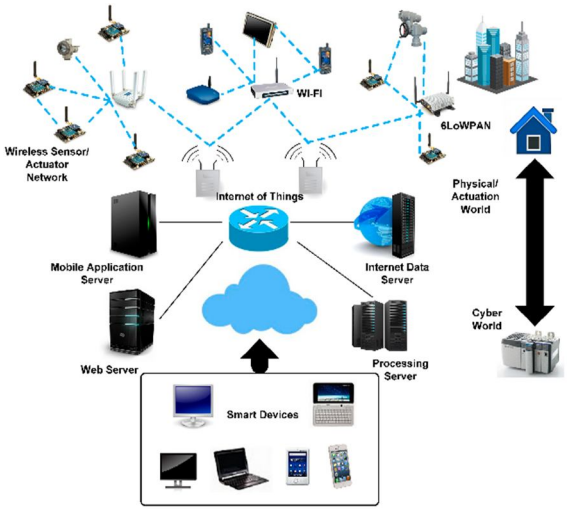


Fig 1: Integration in WSN

II. RELATED WORKS

There are many key management protocols which are proposed for WSN. Eschenauer and Gligor [8] propose a probabilistic key pre-distribution technique to bootstrap the initial trust between sensor nodes. The main idea is to have each sensor randomly pick a set of keys from a key pool before deployment. Then, in order to establish a pairwise key, two sensor nodes only need to identify the common keys that they share. Chan et al. further extended this idea and propose the q-composite key pre-distribution [9]. This approach allows two sensors to setup a pairwise key only when they share at least q common keys. Chan et al. also developed a random pairwise keys scheme to defeat node capture attacks. Carman et al. [5] study the performance of a number of key management approaches in sensor network on different hardware platform. Perrig et al. [10] develop a security architecture for sensor networks (SPINS), where each sensor node shares a secret key with the base station. As two sensor nodes cannot directly establish a secret key, they can use base station as a trusted third party to setup the secret key. In [11], Basagni et al. present a key management scheme to secure the communication by periodically updating the symmetric keys shared by all sen- Title Suppressed Due to Excessive Length 3 sor nodes.

However, this scheme assumes a tamper-resistant device to protect the key, which is not always available in sensor networks. Blundo et al.[12] proposed several schemes which allow any group of t parties to compute a common key, while being secure against collusion between some of them. These schemes focus on saving communication costs while memory constraints are not placed on group members. When t = 2, one of these schemes is actually a special case of Blom's scheme [13]. Availability of some information on the sensor distribution in the field helps to improve the security of the key pre-distribution schemes. Some locationaware schemes are proposed in [14] and [15]. These techniques divide the target field into non-overlapping square areas and randomly deploy the sensors in every area. The exact location of a sensor in any area is unknown, but there is knowledge about the identity of sensors in every area. This information helps to eliminate the dependency of keys between nonadjacent cells.

III. THE AKM SCHEME

We propose authentication and key management scheme for hierarchical clusters in wireless sensor networks. 3.1 Terms and Assumptions Some of the terms and assumptions that are needed for the proposed scheme are as follows: 4 Firdous Kausar, Ashraf Masood, and Sajid Hussain Network Model The WSN consists of a 3-tier architecture consisting of a base station, cluster heads, and cluster members. Base station is a secure and not prone to failure node. It has virtually unlimited computational, communication, and memory resources. Further, it is assumed that base station can transmit directly to every sensor node. Sensor nodes, however, are battery-constrained and inexpensive nodes. They have limited communication, processing and memory storage resources. Each sensor node can act as a cluster head (CH) or a cluster member. The CH is chosen based on a RECA algorithm given below. A cluster member communicates directly with its cluster head (CH); there is no communication between sensors. In other words, there is 1-hop communication between a cluster member and the CH. Further, cluster heads can communicate with each other directly and to the base station. Figure 1 shows a WSN with three clusters. The cluster heads transmit directly to the base station and cluster members communicate with their cluster heads only. Further, there are a few isolated sensors that do not belong to any cluster and they communicate directly with the base station

Identify the Multiple Sink Nodes

Take the optimal value of sink nodes into cluster category and go for hierarchical clustering. Since the hierarchical clustering is the cluster method based on distance, the process of it can be divided into the following steps.

At first, find the similarity among objects and define the distance that can represent the differentiation of them. In this paper, the Euclidean distance that is calculated above is selected to realize the dissimilarity of them. When the objects and have a close relation, the value of is rather small, even close to 0.

Next, produce the hierarchical cluster tree with the linkage function. In accordance with the hierarchical clustering analysis for nodes topology, the distribution for sink nodes can be marked out; this process is shown in cluster nodes according to the matrix and sink nodes number which acts as cluster category;

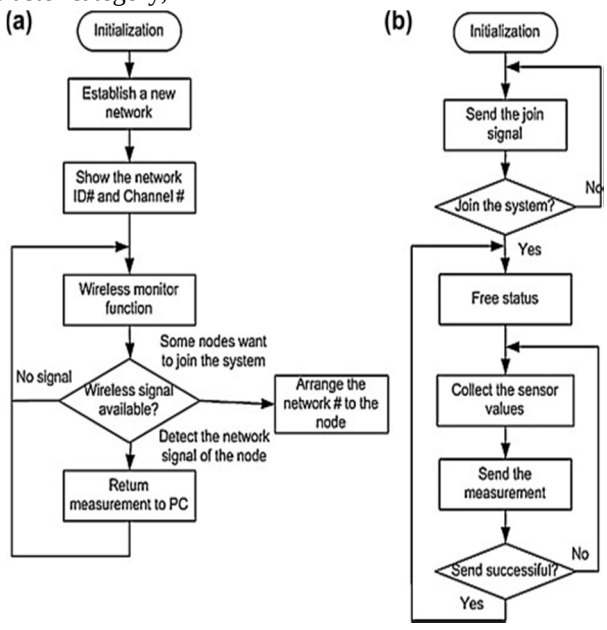
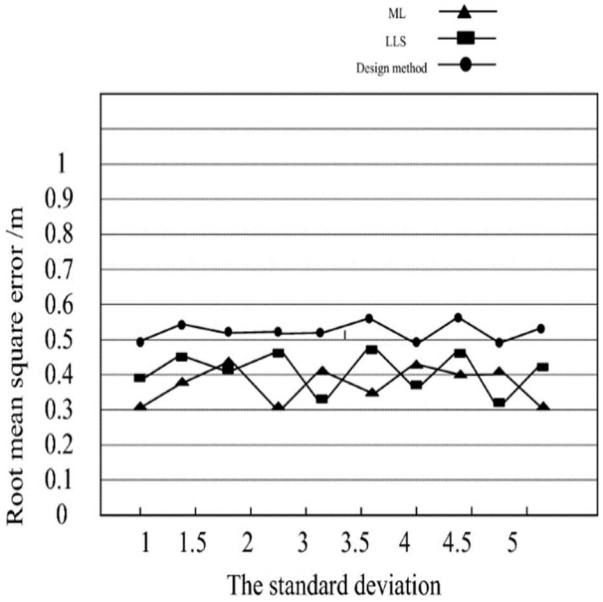


Figure 2

Flow chart for deployment of WSN.

A flag that represents working state will be set up with the help of rand function. If the flag was set to be 0 which means this sink node was dead, the function *up_struct_property(data)* as shown in Algorithm 3 would help to replace the dead sink node with a new one. Then the new sink node was picked up according to the node link distance. If the flag was set to be 1 which means the sink node worked as usual, nothing would be updated for this sink node, and it would continue the node communication.



IV. ENERGY EFFICIENCY MEASUREMENT

The calculation for the energy consumption in the network is processed during the nodes communication. So firstly, the communication source and destination should be identified which concerns the judgment process of the state of sink nodes. Then, work out the calculation method for the energy consumption which is based on the formula for path loss while nodes are communicating. Within the path loss formula, the communication distance is required. And this will be achieved by the weighed shortest routing. Path loss is considered to measure the transmission loss in the topology as the energy consumption per sink node communication. Moreover, with the comparison between the initial energy of the network and total energy consumption, efficiency for the network is sure to be found out and go for optimizing. All the mentioned variables are summarized as follows.

Variables Definition Pl: path loss for one time of communication among the sink nodes; : minimum transmission distance between nodes; : initial energy for the whole network; : energy efficiency of the network.

The energy efficiency of the network is measured by the Pl between communication nodes pair, so the energy efficiency can be worked out as

V. SIMULATION RESULTS

Analysis This section analyzes the proposed scheme and compares it with the other related approaches. Given a WSN, the amount of storage allocated for keys in each node is likely to be a preset constraint, which makes the size of the key ring m a fixed parameter. Once m is set, the choice of S will impact the security level and probability of key sharing among nodes in the network. Given a (S,m)-network, where each node is assigned m keys from a key pool of size S, the security level sl can be defined as follows: sl = 1 − m S (1) which gives the probability that a randomly chosen link is not compromised, when a node that is not either end of the link is compromised. For a fixed m, sl is proportional to S,.

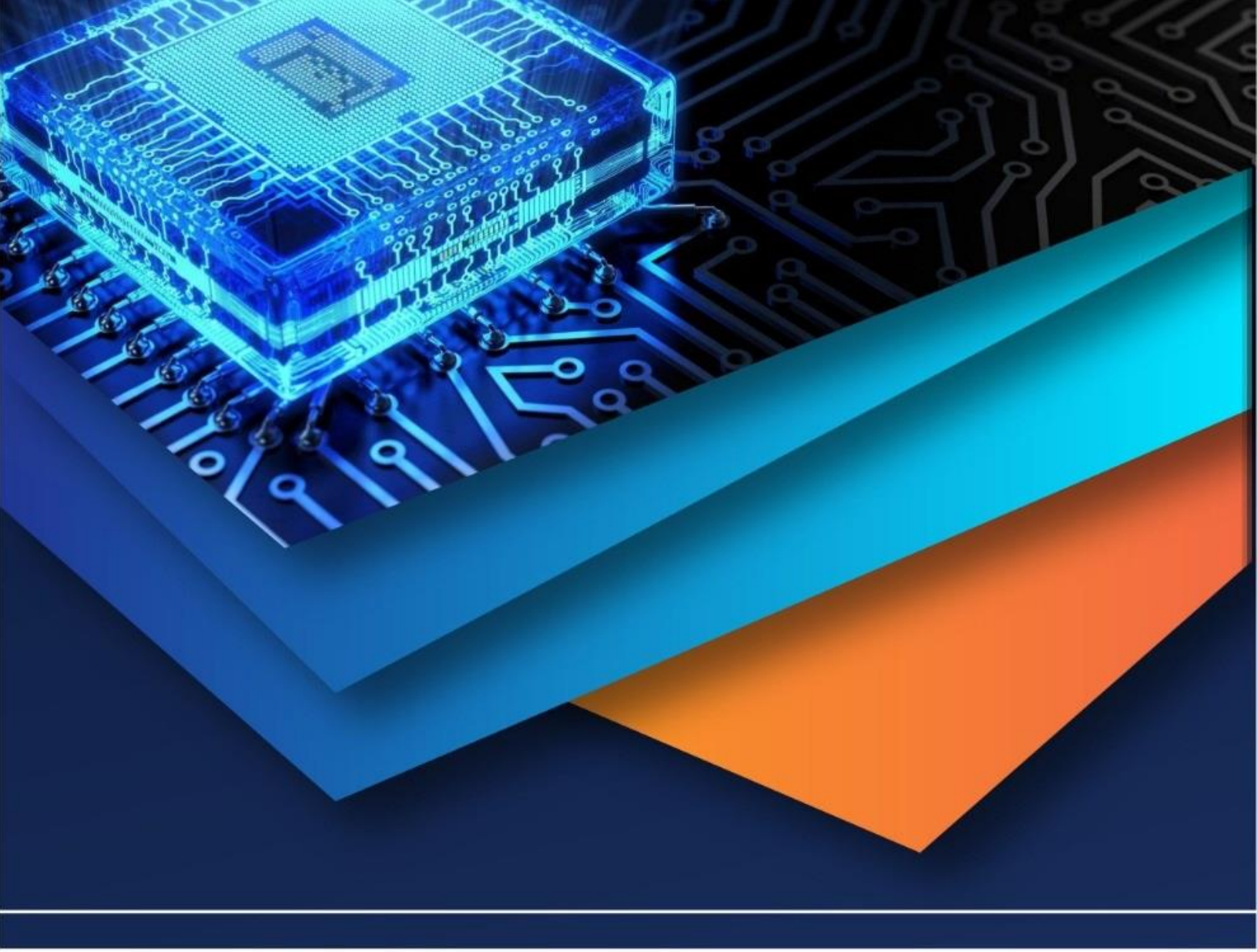
In key distribution schemes, resiliency against node capture measures how much of the network (its communication links) is compromised when a node is compromised. It is a critical performance measure that gauges the robustness of a solution. Our scheme as compared to other random key pre-distribution schemes is more resilient against node capture provided that compromised node re-enter into the network after the epoch in which network key has been refreshed. If a node gets compromised, it is possible for the adversary to know all the keys stored at that node. If we expect that the attacker requires a fixed amount of time to compromise the node, the network key would have changed to new one before the attacker could use the compromise keys.

VI. CONCLUSIONS

The real potential of sensor networks can be fully unleashed if they are connected to the Internet. One of the existing challenges in this area is to assure the existence of certain security properties in the collaboration and integration of sensor networks and Internet hosts. Not only sensor networks should be secure by themselves, but also the interaction between these networks and the Internet should comply with security properties such as confidentiality, integrity, authentication, authorization, accountability, and availability. This paper has reviewed how sensor networks can securely interact with the Internet, and whether existing technology mechanisms are suitable for this scenario. Currently, it is possible to use the base station as a secure front-end proxy that interfaces with the network services, although it is not possible to open a direct channel between hosts and motes, amongst other issues. Other security challenges appear if the sensor nodes are completely integrated into the Internet: creation of end-to-end secure channels, specific protection mechanisms (against denial of service attacks, battery exhaustion attacks, and many others), availability and accountability, sensor node capabilities, and many others. Still, the benefits of integration surely justify the effort of overcoming these challenges.

REFERENCES

[1] Gao, T., Greenspan, D., Welsh, M., Juang, R.R., Alm, A.: Vital signs monitoring and patient tracking over a wireless network. In: The 27th Annual International Conference of the IEEE EMBS, Shanghai, China (2005)
[2] Gu, L., Jia, D., Vicaire, P., Yan, T., Luo, L., Tirumala, A., Cao, Q., He, T., Stankovic, J.A., Abdelzaher, T., Krogh, B.H.: Lightweight detection and classification for wireless sensor networks in realistic environments. In: The 3rd ACM Conference on Embedded Networked Sensor Systems, San Diego, USA (2005)
[3] Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: A survey on sensor networks. IEEE Communications Magazine (2002)
[4] Kahn, J., Katz, R., Pister, K.: Next century challenges: Mobile networking for smart dust. In: The ACM International Conference on Mobile Computing and Networking (MobiCom'99), Seattle, USA (1999)
[5] Carman, D.W., Kruus, P.S., Matt, B.J.: Constrains and approaches for distributed sensor network security. In: Technical report, NAI Labs. (2000)
[6] Zhao, F., Guibas, L.: Wireless sensor networks. Elsevier Inc (2004) 23–24
[7] Li, G., Znati, T.: Reca: a ring-structured energy efficient cluster architecture for wireless sensor networks. International Journal of Sensor Networks 2 (2007) 34–43
[8] Eschenauer, L., Gligor, V.D.: A key management scheme for distributed sensor networks. In: ACM CCS. (2002).
[9] Chan, H., Perrig, A., Song, D.: Random key pre-distribution schemes for sensor networks. In: IEEE Symposium on Security and Privacy. (2003) 197–213
[10] Perrig, A., Szewczyk, R., Tygar, J., Victorwen, Culler, D.E.: Spins: Security protocols for sensor networks. In: Seventh Annual Int'l Conf. on Mobile Computing and Networks. (2001)
[11] Viloria, A., Hernandez-P, H., Lezama, O. B. P., & Orozco, V. D. (2020). Electric Consumption Pattern from Big Data (pp. 479– 485).
[12] Sanchez, L., Vásquez, C., Viloria, A., & Cmeza-Estrada. (2018). Conglomerates of Latin American countries and public policies for the Science (including subseries Lecture Notes inArtificial Intelligence and Lecture Notes in Bioinformatics) (Vol. 10943 LNCS, pp. 759–766). Springer Verlag.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY