iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** XII **Month of publication:** December 2018

DOI:

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: 6.887
Volume 6 Issue XII, Dec 2018- Available at www.ijraset.com

An Energy Efficient Secured Method for Medical Wireless Sensor Networks

Nabil Aslam[1], R. Gowthamani[2], A. Geetha[3]
[1] *PG Scholar,* [2,3] *Assistant Professor, Department of CSE, Nehru Institute of Technology, Coimbatore, India*

Abstract: ***The persistent growth of healthcare requirements has paved the path for finding solutions by integrating various technologies. This paper presents an energy efficient model for securing life saving information with optimal energy consumption in Medical Wireless Sensor Networks (MWSNs). After analysis of the earlier methods, a new method for malicious node detection using hybrid medium access control protocol (HMAC) is proposed for MWSN. In this work, two attacks namely Black hole attack and Sybil attack are concentrated on. In addition, the concept of balanced load is incorporated to reduce the energy consumption of the network. And the concept of sub cluster head selection works for both reduction of energy consumption and also for preventing the network from the black hole and Sybil attack. During performance analysis, various resultant parameters like energy efficiency, energy consumption, packet delivery ratio, packets drop and network delay are effectively calculated.***

Keywords: Energy consumption, energy efficiency, MWSN, sub cluster head selection

I. INTRODUCTION

The advancements in wireless communication technologies enabled deployment of large scale wireless sensor networks (WSNs). Due to the fact that wireless sensor networks are composed of large number of sensor nodes , they have a huge range of applications such as monitoring of environment and rescue missions. In monitoring applications, the event is sensed by the low power sensor node deployed in neighbourhood and the sensed information is transmitted to a remote processing unit or base station. For crucial delivery of information from the environment in real time, it is impossible with wired sensor networks but wireless sensor networks are used for data collection and processing in real time from environment. The ambient conditions in the environment are measured by sensors and then such quantities are processed in order to assess the situation precisely in area around the sensors. Over a large geographical area many sensor nodes are deployed for correct monitoring. Due to the limited radio range of the sensor nodes the increase in network size increases coverage of area but data transmission i.e. communication to the base station (BS) is made possible with the help of intermediate nodes. Depending on the diverse applications of wireless sensor networks they are either deployed manually or randomly. After being deployed either manually or randomly, the sensor nodes self-organize themselves and start communication by sending the sensed information. These sensor networks are deployed at a great rapidity in the existing world. Access to wireless sensor networks through internet is expected within a few years. There is an unlimited potential in this wireless technology with various application areas along with crisis management, transportation, military, patient monitoring, natural disaster, seismic sensing and environmental. In short, two main application categories of wireless sensor networks can be spotted as monitoring and tracking. Of late as the use of wireless devices like smart phones, GPS devices, RFID and other electronic devices have turned into more pervasive and less expensive, the demand for communication and networking among these devices is increased for different applications. The security and performance of a WSN depend on assistance and trust assertion of nodes. A few of the major issues in calculating trust in sensor networks are energy efficiency and extreme computations. The sensor trust model and ambient trust sensor routing use complex Gaussian distribution and location-based routing protocol which deserve computational overhead and more battery consumption. A routing protocol requires more communication resources to decide the best route.

The Addition Encouragement and Multiplication Punishment (AEMP) routing protocol and direct trust dependent link state routing protocol are examples of resource intensive trust-based routing protocols. Policy maker, Keynote, SPKI/SDSI, Role Based Access control (RBAC) are based on role-based trust management language. They specify policies over the nodes, delegating their roles to other nodes when location changes. They identify delegation based only on attributes and not on their identities. Continuation of connectivity and trust are essential criteria in securing link establishment between the nodes. The impact of soaring resource utilization constraints and the varied characteristics of devices in MWSNs make the key management methods inefficient. Thus, to meet the constraints and characteristics of MWSN nodes ,a pervasive authentication protocol and secure data transmission protocol

are employed. The remote anonymous protocol is used to surmount the issues in security provision and Attribute-based encryption schemes along with fuzzy attribute-based encryption schemes address those issues in health care applications. In a remote patient monitoring system, data protection against the insider attacks is a major concern and several processes concerned with cryptographic and attribute based algorithms create not only computational overhead but also consume time. Therefore security assurance with smaller amount of computational overhead and more energy efficiency are chief requirements of MWSNs.

This paper addresses the issues in trust management, and security in MWSNs. The sensor nodes in this architecture can continuously update their configuration and trust level to shun being malicious. They continue to send out usable, private and sensitive information. The 3-tier architecture is based on initial configuration of the wireless sensor nodes. The memory architecture of nodes allows default configuration to be changed. That is why a node can act maliciously when its initial configuration is compromised. The proposed model records the initial configuration and saves it in separate file in an encrypted form and afterwards uses that encrypted file for further processes. The encrypted configuration file is used for energy efficient communication. This is continued until the system is fully trained to identify the trustworthy nodes. The trusted nodes are used in the form of small clusters to ensure random checks by neighbouring nodes.

II. PROPOSED SYSTEM

The balanced load sub-cluster head selection aims to reduce the energy consumption and to increase the life time by introducing load balancing concept in it. If a small number of sub-cluster nodes are heavily loaded, it leads to faster energy consumption and to get normal depletion of energy the balanced load sub cluster head selection is initiated. The distance between the normal child nodes and the sub cluster head plays a main role in energy consumption. So, balanced load sub cluster head selection shows the way to nominal energy reduction of each node present in the network by creating communication with nearer nodes. This is done by means of balanced load among the Sub cluster heads (SCH).

The architecture of proposed network is shown in fig. 1. In the network, the SCH nodes sends hello packets to all the nodes which are present in the surrounding area and the nodes send back the acknowledgement. TDMA MAC scheduling technique is introduced here to avoid collision. According to the receipt of an acknowledgment all SCH nodes compare the distance between itself to the child nodes with the threshold distance. At the end of the distance calculation, each SCH nodes sends the message to the concerned child nodes, which are link with it. If the child receives more than one number of copies then it will randomly select the SCH node which it has to coordinate.

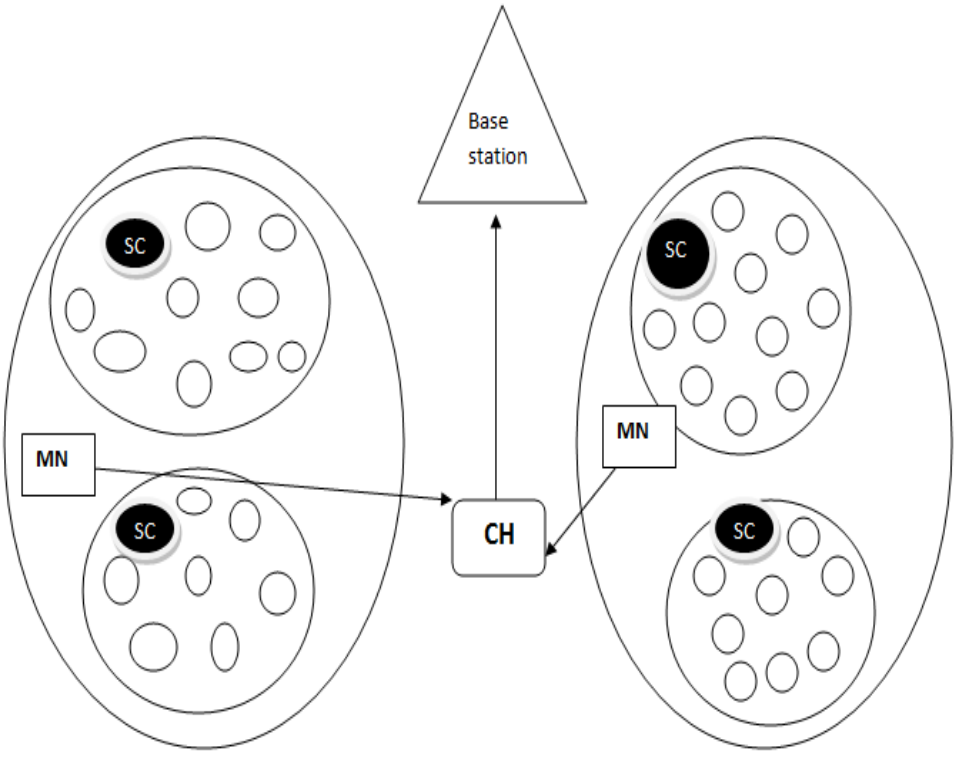


Fig. 1 Architecture of proposed network

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue XII, Dec 2018- Available at www.ijraset.com

Block Diagram

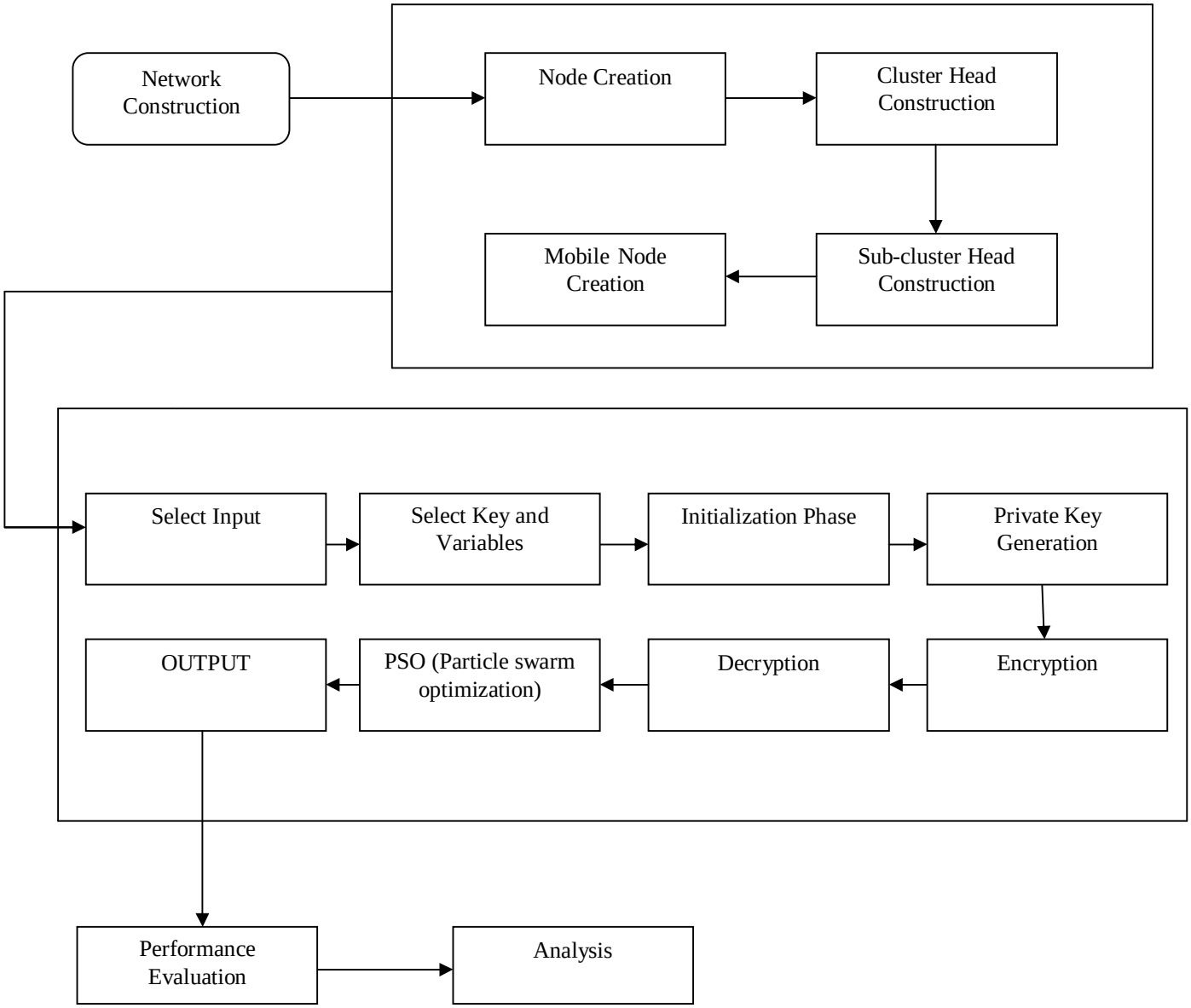


Fig. 1 Block diagram showing the working of proposed method for securing energy efficient transmission

Wireless sensor networks are composed of independent sensor nodes deployed in an area working collectively in order to monitor different environmental and physical conditions such as motion, temperature, pressure, vibration sound or pollutants. The main reason in the advancement of wireless sensor network was military applications in battlefields in the beginning but now the application area is extended to other fields including industrial monitoring, controlling of traffic and health monitoring. Different constraints such as size; cost results in constraints of energy, bandwidth, memory and computational speed of sensor nodes.

A wireless sensor node in a network consists of components such as Microcontroller ,Radio transceiver and Energy source (battery).They can be deployed on large scale. WSNs are scalable and they have the ability to deal with node failures. Another unique feature is the mobility of nodes. They have the ability to survive in different environmental surroundings. They have dynamic network topology. Further developments in this technology have led to integration of sensors, digital electronics and radio communications into a single integrated circuit (IC) package. Generally wireless sensor network have a base station that communicates through radio connection to other sensor nodes.

III.RESULTS AND DISCUSSIONS

The proposed schemes have been experimented in a network deployed with 20 nodes in the simulation environment of NS2. During the communication, the Sybil node is detected which would attack the network by creating multiple identities from same malicious node. Compared with the existing methods, the proposed method detects the Sybil nodes in the initial stage itself ie. while route discovery is being carried out. But in other methodologies, Sybil nodes are detected during the data transmission only.

In Route detection, a network is created with given number of nodes; then each node in the network establishes a route to the sink node by using intermediate relay nodes, after successfully establishing the routes for all the nodes. Select some sender node then send the data to the sink node from the selected sender.

In blackhole detection, experimentally, one node become as a black hole node and the route detection will happen for all the nodes (a blackhole attack is a type of denial-of-service attack in which a router that is supposed to relay packets instead discards them) . Detected routes after the black hole attack are checked by selecting some sender node then sending data.

The simulations are carried out in NS2 simulator. Computational overhead rate, throughput based on trust calculation, energy consumption and data drop rate are calculated and compared with existing algorithms. Results show that proposed model and existing model performed nearly the same in the beginning (till 10 nodes). This is because the nodes in proposed model take some time to form clusters and calculate the trust among them, once clusters are formed and trust relationships are established and proposed model starts performing better. Energy consumption by nodes in proposed model is less as compared to nodes in previous works.

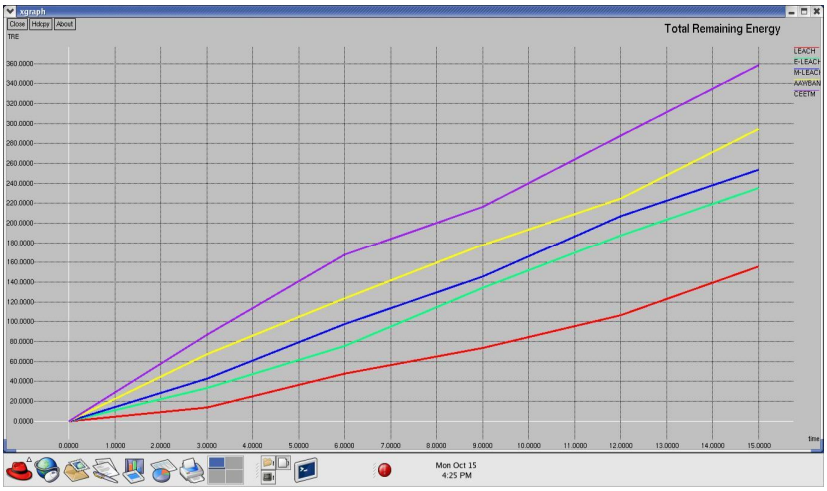


Fig.3 Total TCP Received Packet Calculation of the Network

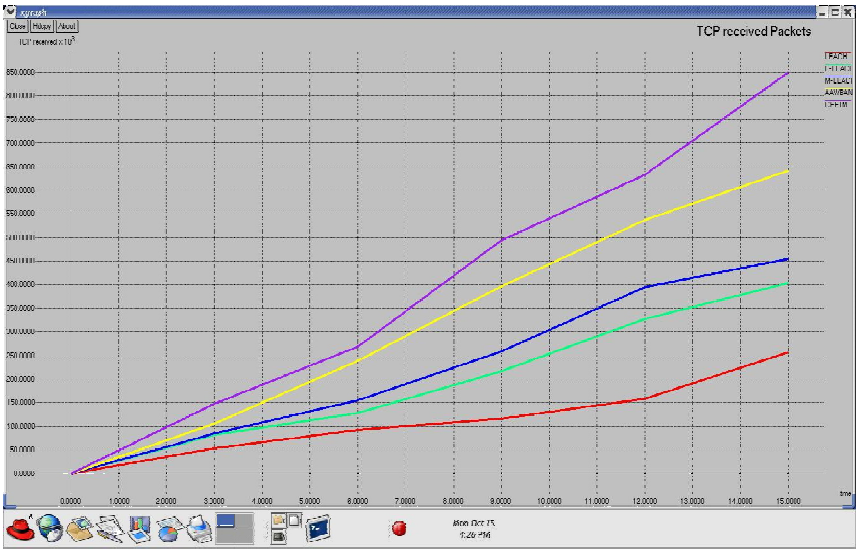


Fig.4 Packet Delivery Ratio Calculation of the Network

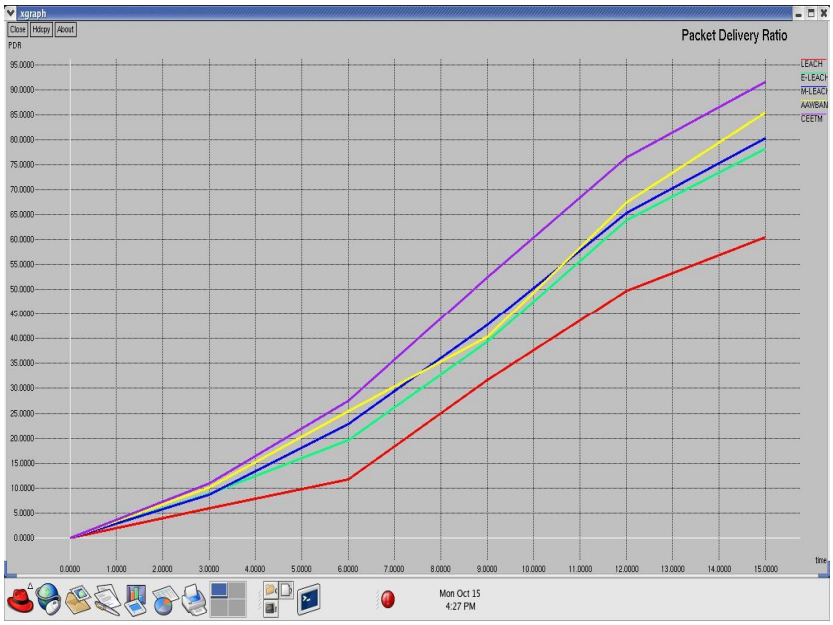


Fig. 5 Average Remaining Energy Calculation of the Network

The snapshots showing the results are clearly understood from figures 3,4 and 5.

IV. CONCLUSIONS

Energy efficiency is an important concern in resource sensitive healthcare sensor based devices. Because of the neglect of this vital parameter several latest technologies have failed to address trust management issues with optimal energy consumption. The proposed model with its architecture and efficient cluster-based computation allowed the network to perform better in terms of computational overhead, data drop rate, energy consumption and throughput. Confidence among nodes is achieved and clustering of nodes allows distribution of computation overhead thereby resulting in a comprehensive energy efficient solution.

REFERENCES

[1] F. Ullah, A. H. Adullah, M. Q. Jan, and K. N. Qureshi, "Patient data prioritization in the cross-layer designs of wireless body area network," Journal of Computer Networks and Communications, vol. 2015, Article ID 516838, 21 pages, 2015. doi: 10.1155/2015/516838 2015.

[2] Gu Xiang, Qiu Jianlina, Wang Jina,"Research on Trust Model of Sensor Nodes in WSNs", in International Workshop on Information and Electronics Engineering (IWIEE), pp.45-57, 2012.

[3]] D. He, C. Chen, S. Chan, J. Bu, and A.Vasilakos, "ReTrust: Attack-resistant and lightweight trust management for medical sensor networks," IEEE Transactions on Information Technology in Biomedicine, vol. 16, no. 4, pp. 623-632, 2012.

[4] M. Somasundaram and R. Sivakumar, "Game Theory Based Security in Wireless Body Area Network with Stackelberg Security Equilibrium". The Scientific World Journal, vol. 2015, Article ID 174512, 9 pages, 2015. doi:10.1155/2015/174512.

[5] X. Qi, K. Wang, A. Huang, H. Hu, and G. Han, "MAC protocol in wireless body area network for mobile health: a survey and an architecture design," International Journal of Distributed Sensor Networks, vol. 11, issue 10. 2015.

[6] C. Hu, X. Cheng, F. Zhang, D. Wu, X. Liao, and D. Chen, "OPFKA: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks," in INFOCOM 2013 Proceedings IEEE, 2013, pp. 2274-2282.

[7] Y. S. Lee, E. Alasaarela, and H. Lee, "Secure key management scheme based on ECC algorithm for patient's medical nformation in healthcare system," in The International Conference on Information Networking 2014 (ICOIN2014), 2014, pp. 453-457.

[8] P. Picazo-Sanchez, J. E. Tapiador, P. Peris-Lopez, and G. SuarezTangil, "Secure publish-subscribe protocols for heterogeneous medical wireless body area networks," Sensors, vol. 14, issue 12, pp. 22619-22642, 2014

[9] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Pauthkey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed iot applications," International Journal of Distributed Sensor Networks, vol. 2014, 2014.

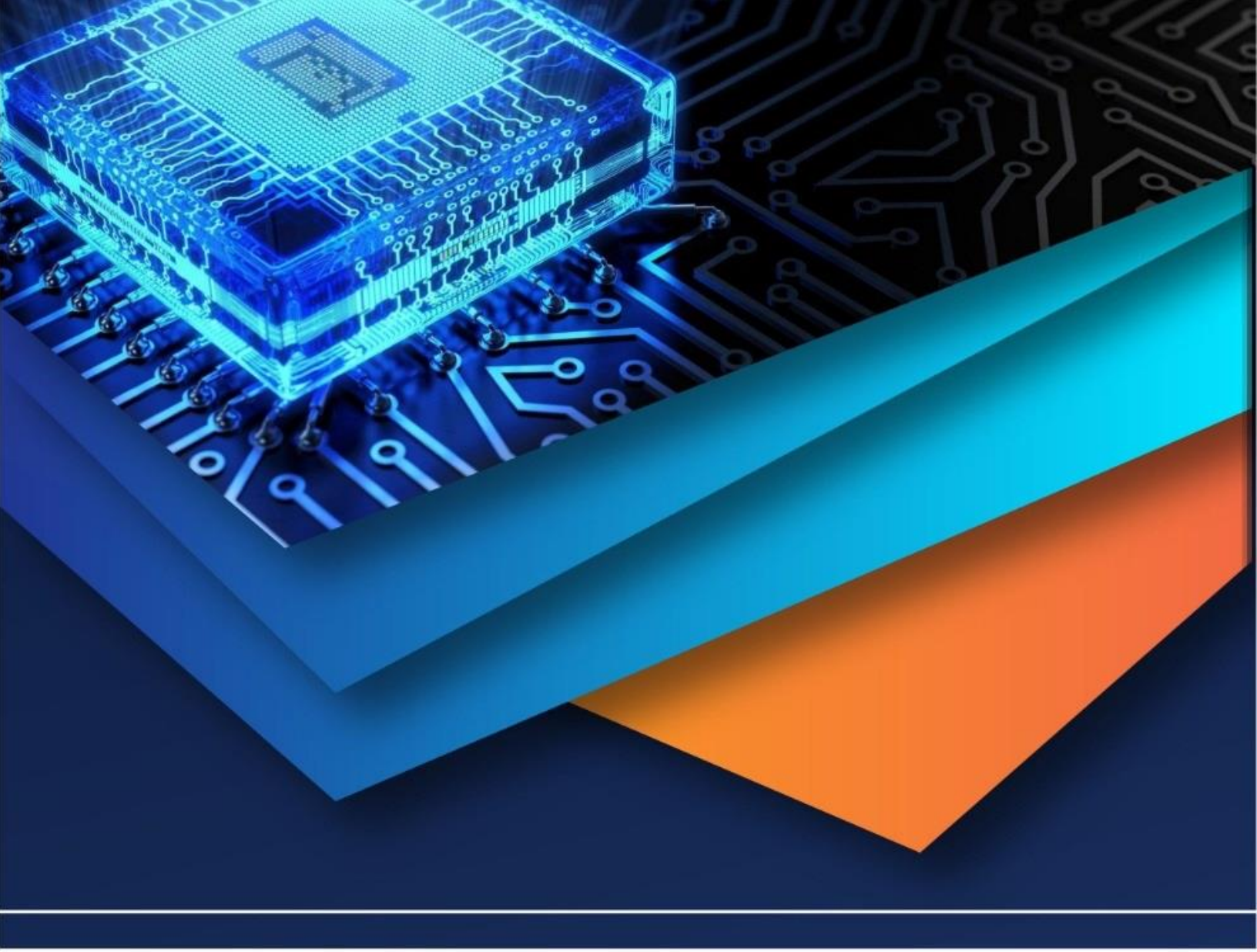
[10] S. B. Othman, A. A. Bahattab, A. Trad, and H. Youssef, "Secure data transmission protocol for medical wireless sensor networks," in IEEE 28th International Conference on Advanced Information Networking and Applications, 2014, pp. 649-656.

[11] M. S. Padma, D. J. W. Wise, M. S. Malaiarasan, and M. N. Rajapriya, "Ensuring Authenticity and Revocability for Wireless Body Area Network using Certificateless Cryptography," International Research Journal of Engineering and Technology, vol. 3, issue 3, pp. 17111715, 2016

[12] C. Hu, F. Zhang, X. Cheng, X. Liao, and D. Chen, "Securing communications between external users and wireless body area networks," in Proceedings of the 2nd ACM workshop on hot topics on wireless network security and privacy, 2013, pp. 31-36.

[13] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attributebased encryption," IEEE transactions on parallel and distributed systems, vol. 24, issue 1, pp. 131-143, 2013.

[14] A. Lounis, A. Hadjidj, A. Bouabdallah, and Y. Challal, "Secure and scalable cloud-based architecture for e-health wireless sensor networks", in 21st International Conference on Computer Communications and Networks (ICCCN), 2012, pp. 1-7.
[15] Y. Tian, Y. Peng, X. Peng, and H. Li, "An attribute-based encryption scheme with revocation for fine-grained access control in wireless body area networks," International Journal of Distributed Sensor Networks, vol. 2014.
[16] M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, "High resolution fiber distributed measurements with coherent OFDR," in Proc. ECOC'00, 2000, paper 11.3.4, p. 109.
[17] R. E. Sorace, V. S. Reinhardt, and S. A. Vaughn, "High-speed digital-to-RF converter," U.S. Patent 5 668 842, Sept. 16, 1997.
[18] (2002) The IEEE website. [Online]. Available: http://www.ieee.org/
[19] M. Shell. (2002) IEEEtran homepage on CTAN. [Online]. Available: http://www.ctan.org/tex-archive/macros/latex/contrib/supported/IEEEtran/
[20] FLEXChip Signal Processor (MC68175/D), Motorola, 1996.
[21] "PDCA12-70 data sheet," Opto Speed SA, Mezzovico, Switzerland.
[22] A. Karnik, "Performance of TCP congestion control with rate feedback: TCP/ABR and rate adaptive TCP/IP," M. Eng. thesis, Indian Institute of Science, Bangalore, India, Jan. 1999.
[23] J. Padhye, V. Firoiu, and D. Towsley, "A stochastic model of TCP Reno congestion avoidance and control," Univ. of Massachusetts, Amherst, MA, CMPSCI Tech. Rep. 99-02, 1999.
[24] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE Std. 802.11, 1997.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY