SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 6 | June 2024 - Peer Reviewed Journal

IMPLEMENTATION OF ENERGY EFFICIENT SECURITY MECHANISMS FOR WIRELESS SENSOR NETWORKS

Sirasani Srinivasa Rao[1], Gajula Madhavi[2], G.Ravi Kumar[3],

[1]*Associate Professor, Department of ECE, Mahatma Gandhi Institute of Technology, Hyderabad, Telangana, India.*
[2]*Associate Professor, Department of ECE, Mahatma Gandhi Institute of Technology, Hyderabad, Telangana, India.*
[3]*Assistant Professor, Department of ECE, Mahatma Gandhi Institute of Technology, Hyderabad, Telangana, India.*

Article DOI: https://doi.org/10.36713/epra17302
DOI No: 10.36713/epra17302

ABSTRACT

Designing energy-efficient security mechanisms is critical for WSNs due to their limited power resources. Techniques like low-power cryptography, duty cycling, and energy-aware security protocols can help in achieving security without significantly impacting the energy consumption of sensor nodes. *In this paper, we propose an energy aware geographical multipath routing scheme for WSNs. The distance to the destination location, remaining battery capacity, and queue size of candidate sensor nodes in the local communication range are taken into consideration for next hop relay node selection, and Analytical Hierarchy Process (AHP) and Geographical Routing Algorithm (GRA) are applied for decision making. Simulation results show that these schemes can extend the network lifetime longer than the original geographical routing scheme which only considers distance to the destination location.*

KEYWORDS: *WSN, linear discriminate packet flow analysis system, optimized rout path switch, Analytical Hierarchy Process (AHP) and Geographical Routing Algorithms(GRA).*

1 INTRODUCTION

Different assaults, for example, listening in, data altering, and malevolent control direction infusion would force a genuine danger on secure and stable savvy lattices activity in the wireless channels. Because of progression in innovation, sensor networks, and wireless correspondence give ascend to another innovation known as wireless sensor networks (WSNs). This innovation is developing quickly as of late. The system works on the wireless medium. This medium is open for all, for example, the odds of a wireless system to be undermined in examination with wired networks are more in WSNs. So the arrangements devoted to the wired system are not adequate for asset compelled wireless sensor arrange. There is as yet a degree for wide inquire about the potential in the field of wireless sensor organize security[1-2]. In this part, we dissect issues identified with security in WSNs and feature investigates destinations actualized in this proposition in the field of wireless sensor networks. WSNs are developing as both a huge new level in the IT environment and a rich space of dynamic research including dispersed calculations, information the board, equipment and framework configuration, programming models, systems administration, security, and social elements. WSN screens the ecological and physical factors, for example, pressure, sound, temperature and so on, with the assistance of self-coordinated sensors that are dissipated over distinctive geological areas. The advanced networks play out the detecting movement along with the two bearings[3-4]. The WSNs are generally utilized in military reconnaissance, which are enacted the augmentation of the sensor networks. The WSN comprise of an immense number of hubs, which are interconnected with each other [5-6].

Every hub in WSN regularly contains the accompanying parts: a microcontroller goes about as a delegate between a wellspring of vitality and the sensor hubs, a radio handset with association with outside or inward reception apparatus. There is a requirement on assets, memory, vitality, correspondence data transfer capacity expense and size of WSN. Sensor networks comprise of many distinctive highlights. The all outnumber of hubs in an customary sensor system is higher than in an ordinary specially [7-8] appointed system. Thick organizations are normally wanted to guarantee better network and high inclusion. Therefore, the sensor modest hubs generally have stringent vitality requirements that make them more disappointment inclined. They are typically thought to be stationary, yet the unstable idea of wireless channels what's more, visit breakdown bring about a variable system topology. In a perfect world, sensor organize equipment must be little, reasonable, control effective, and solid in request to upgrade arrange lifetime, lessen the requirement for upkeep, include adaptability. There is a variety between star topology what's more, a multi-jump work topology as far as basic arrangement of sensor hubs. The sensor hubs are conveyed arbitrarily over the system. Fig 1 shows the multi-jump WSN engineering with various sensor hubs and a portal sensorhub [9-10].

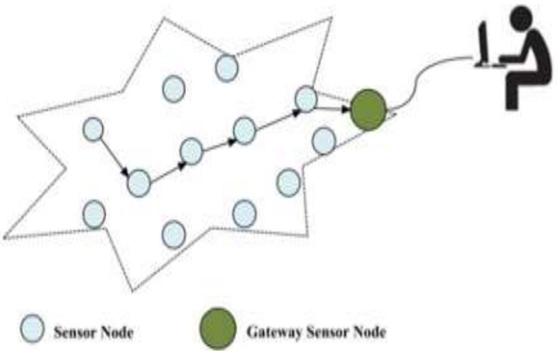

Figure 1 WSNs Multi-hop

Forswearing of-administration from sticking is hard to counteract with the constrained assets accessible to most specially appointed and WSN hubs [11-12]. Hubs may be static once conveyed, and have fixed vitality saves. Radio transmission is a vitality costly activity, yet an aggressor can meddle with it.

The military has since a long time ago managed sticking [13-14] by utilizing spread-range correspondence [15-16]. Be that as it may, the assets required for conventional resistances and the dangers in warfighting are inconsistent with the requirements in WSNs. Past age WSNS utilized single-recurrence radios and are unprotected against narrowband commotion, regardless of whether inadvertent or pernicious. These employments of spread range lessen the effect of narrowband commotion on correspondence, for example, that from microwaves and different wireless networks. Be that as it may, they don't overcome an enemy with learning of the spreading codes or jumping succession. Since these are either institutionalized (in IEEE 802.15.4) or got from hub addresses (in Bluetooth), they are not mystery. While it isn't likely that asset compelled WSNs will have the option to oppose a well- subsidized, ground-breaking wide-band jammer, we accept the bar has been left painfully low. We show that an aggressor ready to bargain a WSN hub can soley through programming cause an overwhelming refusal of-administration. This interfere with sticking assault is vitality effective and stealthy, since it possibly sticks when vital. Further, the aggressor's microchip can rest until the message is recognized by means of an interfere [17-18].

As WSNs move from the lab and controlled conditions into open spaces, their introduction to various types of security assaults develops. Safeguards against such effectively mounted sticking assaults are expected to change the existing security unevenness, regardless of whether arrangements are definitely not impeccable or don't address all classes of assailants [19-20]. Past arrangements center around the troublesome issue of identifying sticking, make troublesome suppositions about hub portability or abilities, don't address sporadic sticking, or are assessed uniquely in reproduction. To the best of our insight, this work is the first to legitimately go up against different sorts of sticking on normal WSN equipment with arrangements that are indicated observationally to enable hubs to keep on conveying regardless of an continuous disavowal of- administration assault [21-22].

SYSTEM MODEL

To accomplish energy-efficiency a proficient system of group head choice is acquainted with limit the cover zone secured by at least one bunch heads. In existing information collection conventions, a solitary example is determined by applying a totaled work on the perusing of all the sensor hubs in a bunch. This activity is performed by the bunch head. There are two downsides of this plan[25-26]. The principal disadvantage is that the measure of information got by the base station is less in light of the fact that the perusing of a few bunch individuals is changed over to a solitary perusing and this single perusing is gotten by the base station from each bunch which influences the general consequences of the group. The second disadvantage of existing secure information total plans is that it breaks the standard of privacy between a sensor hub and the base station on the grounds that the real perusing of a sensor hub is unveiled to the group head. So in introduced information conglomeration conventions, these issues have been tended to appropriately. In first case, rather than sending a solitary collected example from group head to the base station, one example from each copy class is moved from a sensor hub to the base station. This convention likewise keeps up the rule of classification between a sensor hub and the base station as the genuine sensor perusing is escaped the group heads. Rather than sending the real perusing to the group head, the sensor hub sent an example code to the bunch head. This example code is all that anyone could need to analyze the excess among the readings of two extraordinary sensors. This plan additionally gives a security system between sensor hubs and aggregator sensor hub and BS.

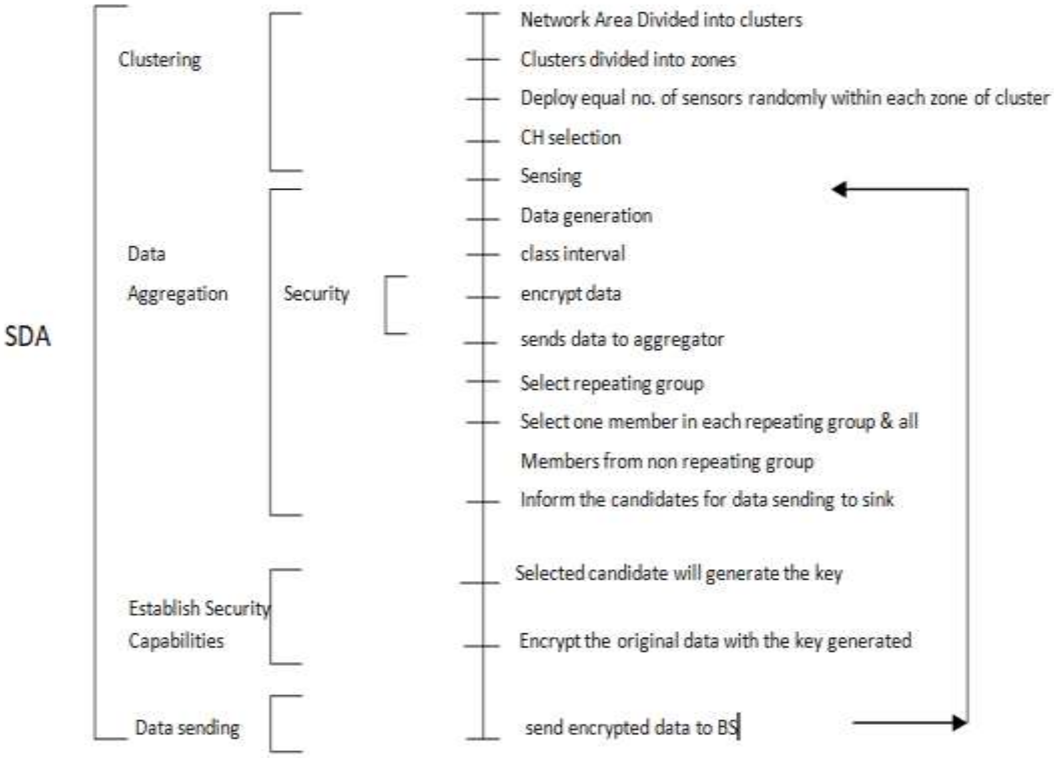
SDA
Clustering
Data
Aggregation
Security
Establish Security
Capabilities
Data sending
Network Area Divided into clusters
Clusters divided into zones
Deploy equal no. of sensors randomly within each zone of cluster
CH selection
Sensing
Data generation
class interval
encrypt data
sends data to aggregator
Select repeating group
Select one member in each repeating group & all
Members from non repeating group
Inform the candidates for data sending to sink
Selected candidate will generate the key
Encrypt the original data with the key generated
send encrypted data to BS

Figure 2: System-Model

Security is a broadly utilized term incorporating the attributes of verification, security, honesty, nonrepudiation and hostile to playback [1]. When contrasted with wired networks, the WSNs are exceptionally inclined to assaults due to asset imperatives on sensor hubs and the communicate idea of the transmission medium. Security confirmation is the significant test in WSNs. In sensor networks, novel difficulties develop in guaranteeing the security of sensor hubs and the information they produce. A sensor system ought not spill sensor readings to its neighbors. The hubs in the WSNs utilized for military correspondence contains delicate information. In a few applications, the hubs disperse the keys that are delicate in nature. Thus, it is basic to build a safe direct in WSN.

Proposed Method

The fundamental objective of security in WSNs is to ensure the data put away in the memory of sensor and furthermore to monitor the data and assets from assaults and bad conduct. Security prerequisites in WSNs are appeared in Fig 3.

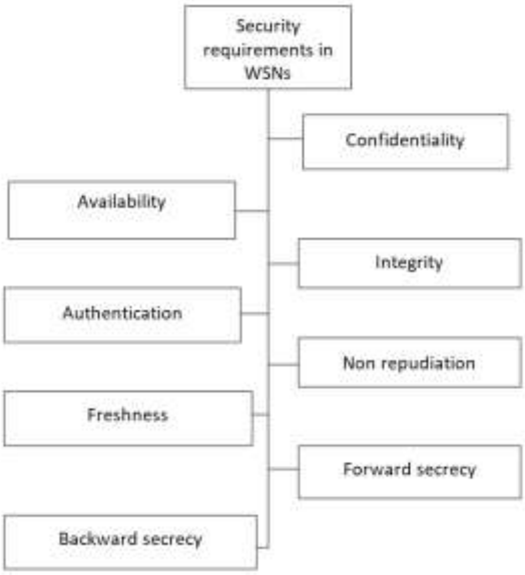

Figure.3. WSN Security requirements

In this part we present a study of information directing calculations and some security related parameters in WSNs. In-arrange collection manages this conveyed handling of information inside the arrange. In this scheme, the sensor network is separated into pre-characterized set of locales every district is answerable for detecting and detailing occasions that happens inside the area to the sink hub. In a run of the mill sensor arrange situation, unique hub gather information from the earth and afterward send it to some focal hub or then again sink which examine.

Be that as it may, in-Network information collection s, information delivered by various hub can be mutually prepared while being sent to the sink hub. Elena Fosolo et al in [8] characterizes the in- arrange conglomeration process as pursues: accordingly expanding system lifetime." In in network accumulation, the sensor with the most basic data totals the information bundles and sends the melded information to the sink. Every sensor transmits its signal solidarity to its neighbors. On the off chance that the neighbor has higher sign quality, the sender quits transmitting parcels. Subsequent to getting parcels from every one of the neighbors, the hub that has the most noteworthy sign quality turns into the information aggregator. The in-organize accumulation plan is most appropriate for conditions where occasions are exceptionally restricted.

EXPERIMENTAL RESULTS

We think about the vitality cost of the beamforming plan with that of a joined helpful conspire which specifically switches between helpful beamforming and agreeable decent variety in light of the geometry of the system to limit the normal vitality.

Two arrangements of reenactments are performed. In the primary arrangement of analyses, we fix the separation between the source and the goal hubs, and take a gander at the presentation of the joined helpful conspire versus agreeable beamforming. We place the source hub at the inside of the system, i.e., at area (0, 0), and put the goal at separation 2 from the source at area (2, 0). The busybody hub is permitted to be in any point in the square system. Fig. 4 answers the primary inquiry presented in the presentation, by demonstrating the meddler areas for which changing to helpful assorted variety brings about vitality reserve funds just as the measure of vitality put something aside for every area. Fig.4 shows the outcomes for various estimations of the parameters α, D and E, to catch the impacts of the three parameters. We see that the consolidated plan can show a critical exhibition improvement getting near 90% vitality reserve funds for some busybody areas.

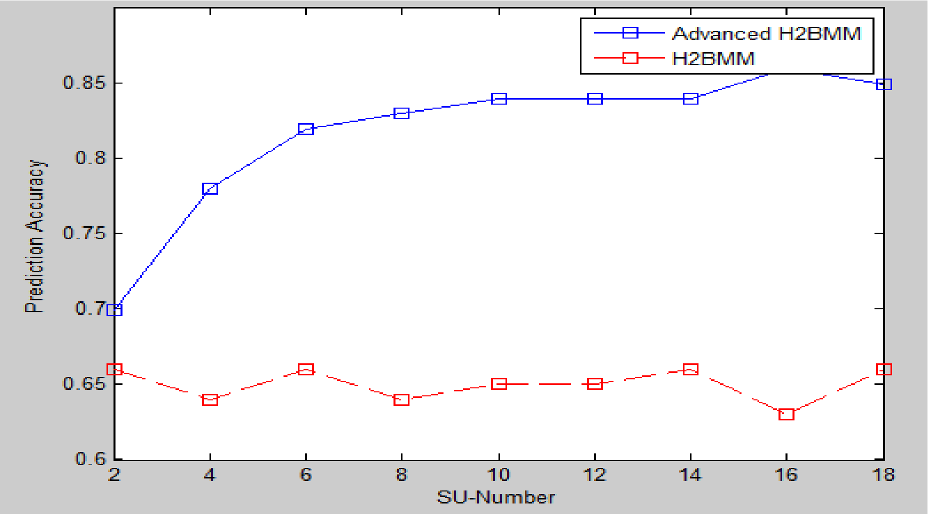

Fig .4: Prediction accuracy

This is the decent variety increase acquired. Other than indicating that agreeable decent variety can be helpful in lessening the transmission vitality in a protected correspondence, Fig. 4 likewise gives knowledge about the geometries where the joined plan shows better execution. Results from the primary arrangement of tests, introduced in Fig. 4, offer response to our first question, as we see that there are a few cases wherein agreeable assorted variety can help to accomplish vitality gains. This perception prompts the second arrangement of investigations, where we ascertain the normal vitality investment funds by the joined helpful plan over all areas of the meddler. Like the principal set of reenactments, the source hub is put at the inside of the square topology. The goal hub is put at various areas along the X-pivot in steps of 0.5 away from the source.

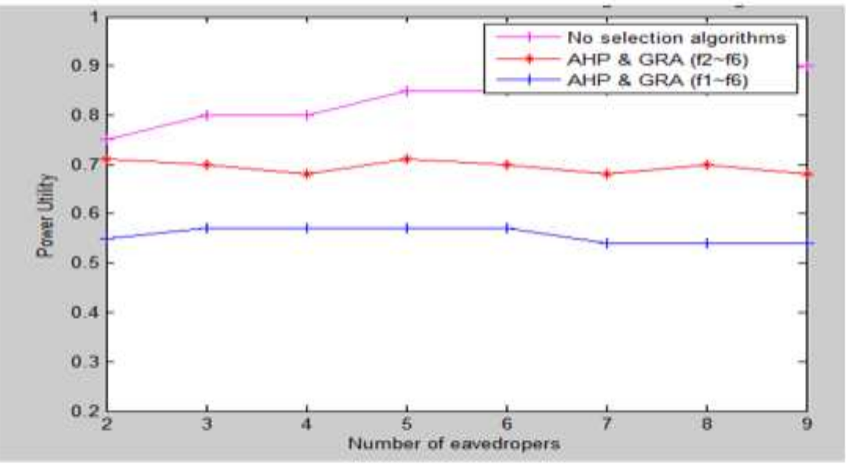

Fig: 5. Power consumption of AHP & GRA versus number of Eavesdroppers

Fig. 5 shows the transmission control versus the quantity of spies around the transmitter. In this figure, $p_{eav} = 10^{-5}$, $r_{min} = 0.01$, $r_{max} = 2$, and dSD = 1. As the power required when utilizing AHP doesn't rely upon the quantity of busybodies. Then again, when the quantity of meddlers builds, the power expected to set up a safe connection utilizing GRA increments significantly. Since the expense of correspondence utilizing AHP just relies upon the separation between the transmitter and the beneficiary which is standardized to dSD = 1, the expense of utilizing AHP doesn't change with the difference in way misfortune type in these plots.

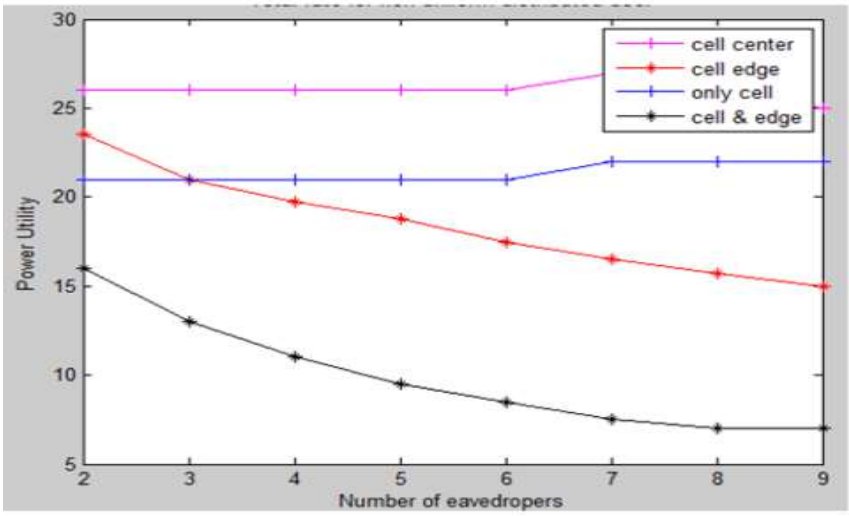

Fig. 6: Power consumption of cells versus the radious r_{min}

Though the proposed calculation (AHP) doesn't require a watchman locale, review that GRA can't be used without such. Fig. 6 shows the control versus r_{min} within the sight of nE = 5 spies, and for different estimations of the way misfortune example α. We set dSD = 1, peav = 10^{-5} what's more, $r_{max} = 2$. We watch that when r_{min} gets little, the power expected to set up a safe connection utilizing GRA increments significantly, while the power expected to set up a protected connection utilizing AHP doesn't rely upon the area of the spy. In certainty as the power utilized by AHP is free of the separation between the transmitter furthermore, the meddlers, and, regardless of whether the spies.

CONCLUSION

In this paper, we have considered secure vitality proficient directing in a semi static multi-way blurring condition within the sight of latent spies. Since the spies are inactive, their areas and CSIs are not known to the real hubs. In this way we searched for approaches that don't depend on the areas and nature of the channels of the spies. We built up a vitality proficient steering calculation dependent on irregular sticking to abuse non-idealities of the spy's collector to give mystery. Our steering calculation is quick (finds the ideal way in polynomial time), and doesn't rely upon the quantity of spies and their area or potentially channel state data.

REFERENCES

1. *I. F. Akyildiz, W. Su, Y. Sankara Subramanian, and E.Cayirci,―Wireless sensor networks:A survey,‖ Computer Networks, vol. 38, no. 4, pp. 393– 422,2002.*
2. *R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley Computer Publishing, 2001,*

pp.326–331.

3. *R. L. Pickholtz, D. L. Schilling, and L. B. Milstein,—Theory of spread spectrum communications – a tutorial,‖ IEEE Transactions on Communications, vol. 20, no. 5, pp. 855–884,1982.*
4. *Chipcon AS, subsidiary of Texas Instruments, CC1000 and CC2420 Radio Transceiver Products,U,*
5. *J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. E. Culler,and K.S.J.Pister,—System architecture directions for networked sensors,‖ in Proc. of ASPLOS, 2000, pp.93–104.*
6. *Crossbow Inc., MICAz Wireless Sensor Network Hardware,*
7. *J.Polastre, R.Szewczyk, and D.Culler,—Telos: enabling ultralow power wireless research, in IPSN, 2005, pp.364–369.*
8. *Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs), IEEE 802.15.4-2003 Standard for Information Technology, 2003.*
9. *R.M.Kling, Intelmote: an enhanced sensor network node,‖ in Int'l Workshop on Advanced Sensors, Structural Health Monitoring, and Smart Structures,2003.*
10. *Wireless MAC and PHY Specifications for Wireless Personal Area Networks (WPANs),IEEE 802.15.1-2005 Standard for Information Technology, 2005, (Bluetooth).*
11. *Md Abdul Azeem, Khaleel-ur-Rahman khan,A. Pramod,—Security Architecture Framework and Secure Routing Protocols in Wireless Sensor Networks-Survey‖, in International Journal of Computer Science & Engineering Survey (IJCSES), Vol.2, No.4, pp. 189-204, November2011.*
12. *XLuo, XuJi and Myong-Soon Park,—Location privacy against traffic analysis attacks in wireless sensor networks‖, in International Conference on Information Science and Applications (ICISA), Seoul, Korea, Vol. 1, No. 6, pp. 1–6, 21-23 April, 2010.*
13. *Tamara Bonaci, Linda Bushnell and Radha Poovendran,—Node capture attacks in wireless sensor networks: A system theoretic approach‖, in 49th IEEE Conference on Decision and Control (CDC), Atlanta, Georgia, USA, Vol. 1. pp. 6765–6772, 15-17 December 2010.*
14. *Bhoopathy,V. and R.M.S.Parvathi,—Energy Constrained Secure Hierarchical Data Aggregation in Wireless Sensor Networks‖, in American Journal of Applied Sciences, ISSN 1546-9239, Vol.9, No.6, pp. 858-864,2012.*
15. *Alvaro Araujo, Javier Blesa, Elena Romero and Daniel Villanueva,—Security in cognitive wireless sensor networks - Challenges and open problems‖, in EURASIP Journal on Wireless Communications and Networking 2012, (2012):48, February2012.*
16. *Kalyani,P. and C.Chellappan.,—Enhanced RSA CRT for Energy Efficient Authentication to Wireless Sensor Networks Security‖, American Journal of Applied Sciences, Vol. 9, No. 10, pp. 1660-1667, 2012.*
17. *S.Prasanna and S. Srinivasa Rao,—An Overview of Wireless Sensor Networks Applications and Security, in International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Vol. 2, No. 2, May2012.*
18. *Xiaokang Xiong, Duncan S. Wong and Xiaotie Deng,—Tiny Pairing:A fast and light weight pairing- based cryptographic library for wireless sensor networks‖, in Proceedings of the IEEE Wireless Communications and Networking Conference2, IEEE explore Press, Sydney, pp: 1-6, April 18-21,2010.*
19. *Arvinderpal S. Wander, Nils Gura, Hans Eberle, Vipul Gupta and Sheueling Chang Shantz,—Energy analysis of public-key cryptography for wireless sensor networks‖ in Proceedings of the 3rd IEEE International Conference on Pervasive Computing and Communications, PERCOM-2005, pp. 324-328, March 8-12,2005.*
20. *Haowen Chan, Adrian Perrig and Dawn Song, —Random key pre distribution schemes for sensor networks‖, in IEEE Symposium on Security and Privacy, Berkeley, California, ISSN: 1081-6011, PrintISBN:0-7695-1940-7,pp.197–213,11-14 May 2003.*
21. *Laurent Eschenauer and Virgil D. Gligor, —A key-management scheme for distributed sensor networks‖, in Proceedings of the 9th ACM Conference on Computer and Communications Security, pp. 41–47, November 18–22, 2002.*
22. *Kumar, D. S., Kumar, C. S., Ragamayi, S., Kumar, P. S., Saikumar, K., & Ahammad, S. H. (2020). A test architecture design for SoCs using atam method. International Journal of Electrical and Computer Engineering, 10(1), 719.*
23. *Soumya, N., Kumar, K. S., Rao, K. R., Rooban, S., Kumar, P. S., & Kumar, G. N. S. 4-Bit Multiplier Design using CMOS Gates in Electric VLSI. International Journal of Recent Technology and Engineering (IJRTE) ISSN, 2277-3878.*
24. *Saikumar K, Rajesh V, Hasane Ahammad S K, Sai Krishna M, Sai Pranitha G, Ajay Kumar Reddy R, Cab for Heart Diagnosis with RFO Artificial Intelligence Algorithm , International Journal of Research in Pharmaceutical Sciences: Vol. 11 No. 1 (2020)*
25. *V Saikumar, K., Rajesh "A novel implementation heart diagnosis system based on random forest machine learning technique "International Journal of Pharmaceutical Research 12, 3904–3916*
26. *Saikumar, K., and V. Rajesh. "Diagnosis of Coronary Blockage of Artery using Mri/Cta Images Through Adaptive Random Forest Optimization." Journal of Critical Reviews 7.14 (2020): 591-600.*
27. *Devaraju, VSN Kumar, and Sirasani Srinivasa Rao. "A Real and Accurate Vegetable Seeds Classification Using Image Analysis and Fuzzy Technique." Turkish Journal of Physiotherapy and Rehabilitation 32: 2.*