iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** IV **Month of publication:** April 2019

DOI: https://doi.org/10.22214/ijraset.2019.4136

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 7 Issue IV, Apr 2019- Available at www.ijraset.com

An Improved Approach in Malicious Node Detection using HMAC Balanced Load Sub Cluster Head Selection for WSN

Sneha K S[1], G Saran Raj[2]
[1]*Master Of Engineering, Dept. of CSE, Dhanalakshmi Srinivasan College Of Engineering, Coimbatore, India*
[2]*Assistant Professor, Dept. of CSE, Dhanalakshmi Srinivasan College Of Engineering, Coimbatore, India.*

Abstract: ***Wireless Sensor Network played a vital role in several sectors. But still there is a research gape in the area of energy efficiency and privacy issues in WSN. After the analysis of earlier methods, to avoid those issues a new prototype was created called as Advanced Malicious Detection using HMAC Balanced load Sub Cluster Head Selection for WSN. In the network it concentrated two attacks namely Black hole attack and Sybil attack. And also to reduce the energy consumption of the network the concept of balanced load is incorporated with hybrid medium access control protocol. And the concept of sub cluster head selection works for both reduction of energy consumption and also to prevent the network from the black hole and Sybil attack. During the performance analysis the results like energy efficiency, network end to end delay, reliability, integrity, confidentiality, packet delivery ratio, network throughput, energy consumption, packet loss are calculated.***
Keywords: HMAC, SCH, WSN, ECCDH, ECM, Public key, Private key.

I. INTRODUCTION

Sensor network comprises of various recognition stations called sensor nodes, each has little size, light weight and moveable. A WSN is a gathering of remarkable transducers with an interchanges base for observing and recording conditions at shifted areas. Sensors watch, for example, temperature, mugginess, weight, wind discovery, speed, and vibrations and so on. Real uses of sensor systems comprise in the field of Automated and stylish homes, Video investigation, Traffic control, Industrial computerization and so on. Sensor nodes are frequently sent into unpleasant environment, where sensors are opened and unprotected from physical attack. Attack can happens from any heading on any node in a sensor arrange.

Execution of security strategy into a WSN and in this way; security turns into the significant cause. A WSN may comprise of couple of hundreds to a great many sensor nodes.

The sensor node adornment incorporates a micro- controller, a radio collector by the side of receiver wire, a vitality source, an electronic circuit, and a battery. The extent of the sensor nodes can likewise differ from the measurement of a shoe box to as moment as the measurement of a piece of tidy. In that capacity, their costs additionally run from a couple of rupees to several dollars relying on the target of a sensor like vitality usage, data transmission, memory and computational speed rate. Essentialness's utilize and resource usages are main problems, yet security in like manner transforms into a key fundamental. In the WSNs, a couple of irregularities can happen as a result of their nonattendance of taking care of and passing on capacity, confirmed limit restrain, extend, information exchange limit and imperativeness.

One of the critical issues with WSN is to look after security. A WSN should not spill out any of its capability despite when sensors are examined by their neighbor node.

They use encryption estimations for insurance conservation. Finally, on thought it derives that there is a need to find particular enthusiastic segment protection approach in perspective of framework development condition, security level of current event and midway node for different applications.

Trust in WSNs is assessed periodically based on the number of failed and successful communication attempts by a certain node in specific interval of time. The issue with this recursive method of trust estimation technique is that it emphases more on recent state of the node and does not consider any previous failed communication attempts. Consequently, a malicious node can simply eliminate any bad reputation by using some verified successful communications and the later continue to attack. For example, in an on-off attack, the malicious node changes its behavior from good to bad and from bad to good rendering itself undetectable during the attack. Detection of such a state is important to avoid wastage of resources if more nodes behave like this.

©IJRASET: All Rights are Reserved

II. EXISTING SYSTEM

The existing model presents an energy efficient trust management model for securing life-saving information with optimal power/energy consumption by sensor nodes. This model is a cluster based 3 tiers- architecture where first tier records the first-run configuration of the nodes. The second tier secures the data between the nodes, and the third tier ensures energy efficiency by calculating energy consumption at every level and rotates cluster head among the nodes. The simulation results shows smooth functioning of the network with less energy consumption. This scheme performs better than Anonymous Authentication for Wireless Body Area Networks with Provable Security (AAWBAN) in terms of computational overhead, energy consumption, throughput and data drop rate.

In this model, for every entry Attribute-Value pair (AVP) is encrypted during the first execution. The encryption of the AVP is performed by adding another tag consisting of node ID and this can be represented for first tier architecture-node registration. For second tier architecture clustering, in order to divide the computation overhead over the network we have proposed clusters of closely related nodes based on the distance and signal strength. Each cluster is headed by a cluster head (CH) which takes most of the computation and stores the configuration file of all the nodes. When energy consumption goes beyond the set limit the cluster head configuration is sent to another node. This divides the overhead and maintains energy efficiency. At last, for third tier architecture-energy efficiency, energy efficiency is the overall requirement and the proposed algorithm keeps on calculating it and when energy consumption reaches the defined limit a new CH is assigned. New CH assignment depends upon the trust value of the node. In order to become a CH the node has to achieve a certain level of trust.

III. PROPOSED SYSTEM

After analysis the earlier methods, to avoid those issues a new prototype called as Advanced Malicious Detection using HMAC Balanced load Sub Cluster Head Selection for WSN have created. In this model, the network was concentrated on various hybrid attacks namely Black hole attack, Sybil attack, Flooding and Wormhole attacks. The distance between the normal child nodes and the sub cluster head plays a major part in energy consumption. So, balanced load sub cluster head selection leads to nominal energy depletion of each node is present in the network by creating transmission with closer nodes by balanced load among the Sub cluster heads (SCH). The concept of sub cluster head selection works for both reduction of energy consumption and also to prevent the network from the black hole and Sybil attack. In addition to that ECC algorithm and SHA-5 algorithm is combined to provide duel authentication mainly to concentrate the integrity and confidentiality.

IV. SYSTEM WORK FLOW

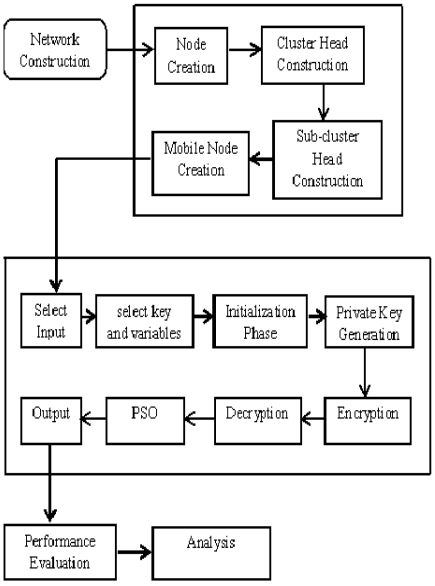


Figure 1 : system working overview

©IJRASET: All Rights are Reserved

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

V. IMPLEMENTATION

A. Balanced Load Sub-cluster Head Selection

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 few 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 major part in energy consumption. So, balanced load sub cluster head selection leads to nominal energy depletion of each node is present in the network by creating transmission with closer nodes by balanced load among the Sub cluster heads (SCH).

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.

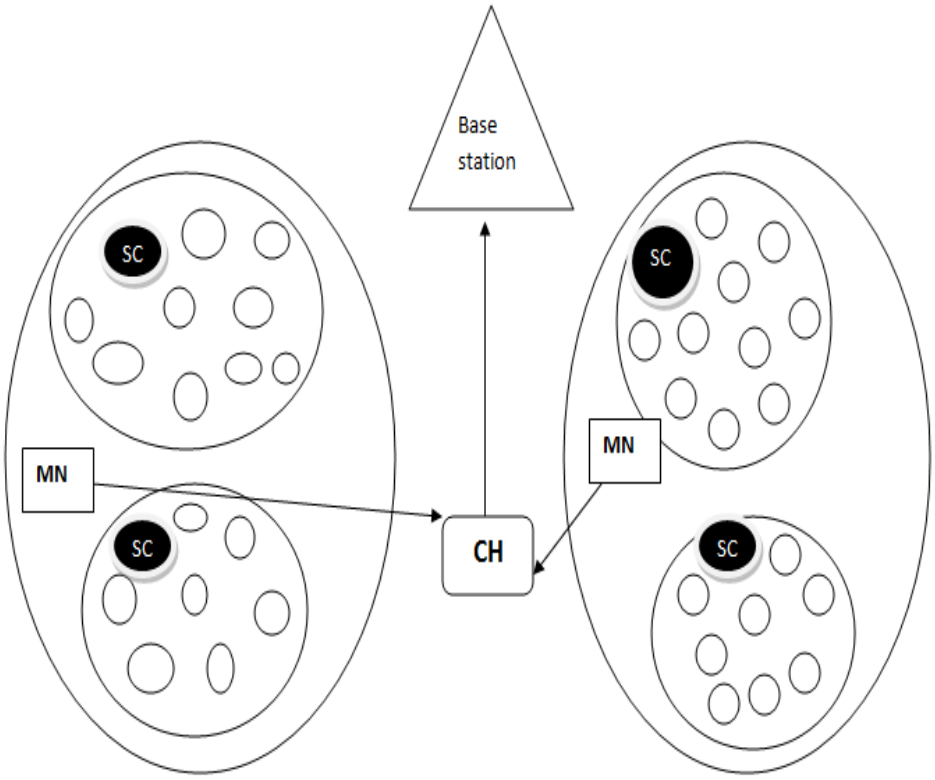


Figure 2: Architecture of proposed network

Along with the network, the balanced load concept is applied to SCH nodes, where the balanced load SCH is formed in each clusters. According to figure 1 shortest distance between the SCH nodes and the child nodes and the distance is calculated using the equation 1. In the figure the black filled circles indicated the SCH nodes and the other nodes are child nodes. The Major Cluster Head (MCH) and the Base Station (BS) are located so far from the field where the nodes are localized. Here Mobile Sink Nodes (MSN) is introduced to collect the information from the SCH and it will transfer it to the MCH node.

$$DISTANCE_{(SCH)(CN)} = \sqrt{SCHi(x,y) - CNj(x,y)} \quad \ldots\ldots\ldots(1)$$

Where i – 1,2,3,…… 10% of the total nodes

j – 1,2,3,……80% of the total nodes

SCH – sub cluster head

CN – child node

$DISTANCE_{(SCH)(CN)} < DISTANCE_{Threshold}$

©IJRASET: All Rights are Reserved

B. Flow chart for Balanced Load Sub-Cluster Head Selection

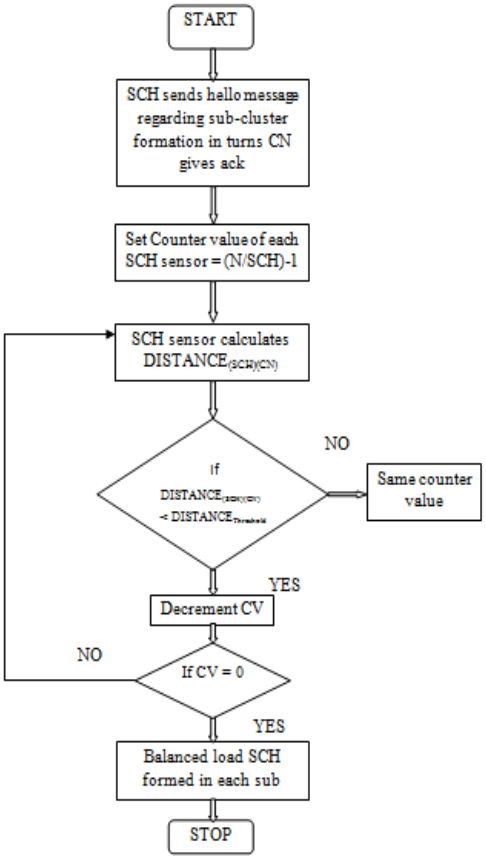


Figure 3: Flowchart of proposed network

C. Algorithm For Balanced Load Sub-Cluster Head Selection

1) Step 1: SCH advertisement and the counter value is declared as (N/SCH)-1 to all SCH nodes.
2) Step 2: CN nodes acknowledgement
3) Step 3: Eq.1 used to calculate SCH and CN distance with $DISTANCE_{Threshold}$.
4) Step 4: If $DISTANCE_{(SCH)(CN)} < DISTANCE_{Threshold}$, decrement the counter value. Else, counter value remains same
5) Step 5: If CV – 0, Stop comparing
6) Step 6: If SCH reaches CL (capacity limits) rejection information transmission starts.
7) Step 7: Rejected CN nodes will send the requests to nearby SCH node.

D. Data Transfer Details

1) Step 1: Child node will transmit the information to the sub cluster head
2) Step 2: The sub cluster head node cannot able to transfer the information directly to the cluster head due to the distance. To address this issues mobile sink nodes are introduced. The mobile sink mode will act as the intermediate between the sub cluster head and the cluster head. It moves from one place to another and collects the information from the sub cluster head and transmits that to the cluster head.
3) Step 3: Each sub cluster consists of one or more mobile sink nodes according to the number of child nodes present in the sub cluster head. If any of the mobile sink efficiency is reduces in that case that sub cluster head will get the help of the neighbor sub cluster head's mobile sink node to transfer the data to the cluster head.

E. Attack Construction Cases

1) Step 1: When child node acts Malicious
2) Step 2: When Mobile sink acts malicious

©IJRASET: All Rights are Reserved

F. H-MAC Mechanism

The mechanism implicated in this Hybrid Medium Access Control protocol involves a step by step procedure after localization process and they are as follows:

1) *Step 1:* Initially the nodes starts to identify the best intermediate node from the location. This is possible by the propagation of hello message from time to time. The exchange of hello message is done every 30sec in this simulation. And the hello memory is then exchanged between nodes, thus enabling the nodes to find the next neighbor and the details are stored in the neighbors list.
2) *Step 2:* Secondly, the node starts to sense their relevant parameters and transmits the data to the destination using CSMA methodology. This process is continued until two conditions. They are:

a) There should be no increase in traffic load and
b) During the absence of emergency packet transmission.

3) *Step 3:* Thirdly, high priority region based data transmission is initiated. If any node is identified that it is in the high priority region, those neighbor nodes holds the data and shifted over to TDMA and provides the current slot to the node which is in the high priority region.
4) *Step 4:* Finally, if two nodes occupies the high priority region in the current slot, then that will be assigned to transfer the information one after the other. At the end CSMA mode will be activated.

G. Duel Authentication Using ECCDH

ECC algorithm and SHA-5 algorithm is combined to provide duel authentication mainly to concentrate the integrity and confidentiality.

1) *Section 1:* ECM - Elliptic Curve method: Elliptic curve method is a cryptography method and it is a part of ECC for the execution of open key cryptography. In the Elliptic curve logarithm the security originates. The block diagram for proposed ECM method is given below.

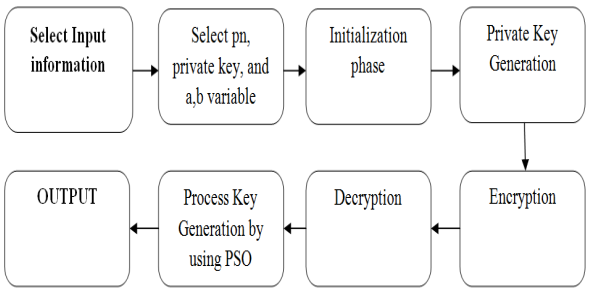


Figure 4: Block Diagram for Proposed ECM Method

H. Parameter Selection Process for ECM method

Curve Equation = $Y^2 \bmod p = X^3 + aX + b \bmod p$ …..(2)

Where, (a, b) are integers and p = prime number.

I. Initialization Phase

In ECM cryptography, the prime number is k and private key is P. Then the equation becomes,

$E = S(i)^3 + u * S(i) + v$ ……..(3)

Where, u and v are constant values and u = v = 2

The smaller key size and reduced storage are the primary benefits which are promised by ECM method. In general, only if the condition X = Y is satisfied that is the best selected point in elliptic curve. The X and Y is

$X = mod\ (E,p_n)$ ……(4)

$Y = mod\ ((S(j))^2, p_n)$ ……(5)

J. Key Generation

The user creates the secret key K_s. Since two keys are created in ECM method which is private key (PR_k) and public key (PU_k). The secret key is under gone XOR operation. The best point $K_s(k,l)$ and PU_k is the public key, then the PU_k is given as,

$$PU_k = PR_k * K_s \quad \text{……(6)}$$

©IJRASET: All Rights are Reserved

K. Encryption Method

Authorization based encoding of messages or information is termed as Encryption. In this process, two points are given as inputs. The data $L_x(n,m)$ and $L_y(n+lm)$ then the point is,

$$G_1 = PR_k * K_s \ldots\ldots(7)$$

$$G_2 = (L_x, L_y) + G_1 \ldots\ldots(8)$$

L. Decryption Method

The reverse methodology of encryption is called decryption which is the process of shifting the of encrypted cipher text to the unique plain text. The private key PR_k is employed to decode the message.

$$G_D = PR_k * G_1 \ldots\ldots(9)$$

In this decryption process the secret key PR_k is generated by the use of different optimization methods such as Genetic algorithm and PSO.

VI. CONCLUSION

In this approach detection and prevention of black hole and sybil attack happens by utilizing the powerful transmission mode. In the event that a solitary attacks is available in the system that can likewise be distinguished and forestalled by this approach. In this exploration paper it dissects the customary HMAC steering convention with attack assault and proposed an answer against its location issue utilizing modified method. In modified transmission force of every node measure by new field. For the counteractive action or security perspective it will document classification and validness to the honest to legitimate node of the system.

The balanced load sub-cluster head selection reduces the energy consumption and increases the life time by introducing load balancing concept in it. If few 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.

REFERENCES

[1] Ms. Gauri P. Heda and P. P. Rokade, " Cluster Based Secure Dynamic Keying Technique For Heterogeneous Mobile Wireless Sensor Networks" International Journal of Innovative Research and Advanced Studies (IJIRAS) Volume 4 Issue 8, August 2017

[2] V. K. Verma, "Pheromone and Path Length Factor-Based Trustworthiness Estimations in Heterogeneous Wireless Sensor Networks," in IEEE Sensors Journal, vol. 17, no. 1, pp. 215-220, 2017

[3] 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.

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

[5] C. Hu, N. Zhang, H. Li, X. Cheng, and X. Liao, "Body area network security: a fuzzy attribute-based signcryption scheme," IEEE journal on selected areas in communications, vol. 31, issue. 9, pp. 37- 46, 2013.

[6] J S Rauthan and S Mishra, " An Improved Approach in Clustering Algorithm for Load Balancing in Wireless Sensor Networks" International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 5, July 2012

[7] B. Deosarkar, N. Yadav and R. P. Yadav, "Clusterhead Selection in Clustering Algorithms for Wireless Sensor Networks; A Survey," In Proc. Int. Conf. Computing, Communication and Networking (ICCCN 2008), Dec 18-20, 2008, Karur, Tamilnadu, India.

[8] Abbasi, M. Younis, "A survey on clustering algorithms for wireless sensor networks," vol. 30, 2007, pp. 2826-2841.

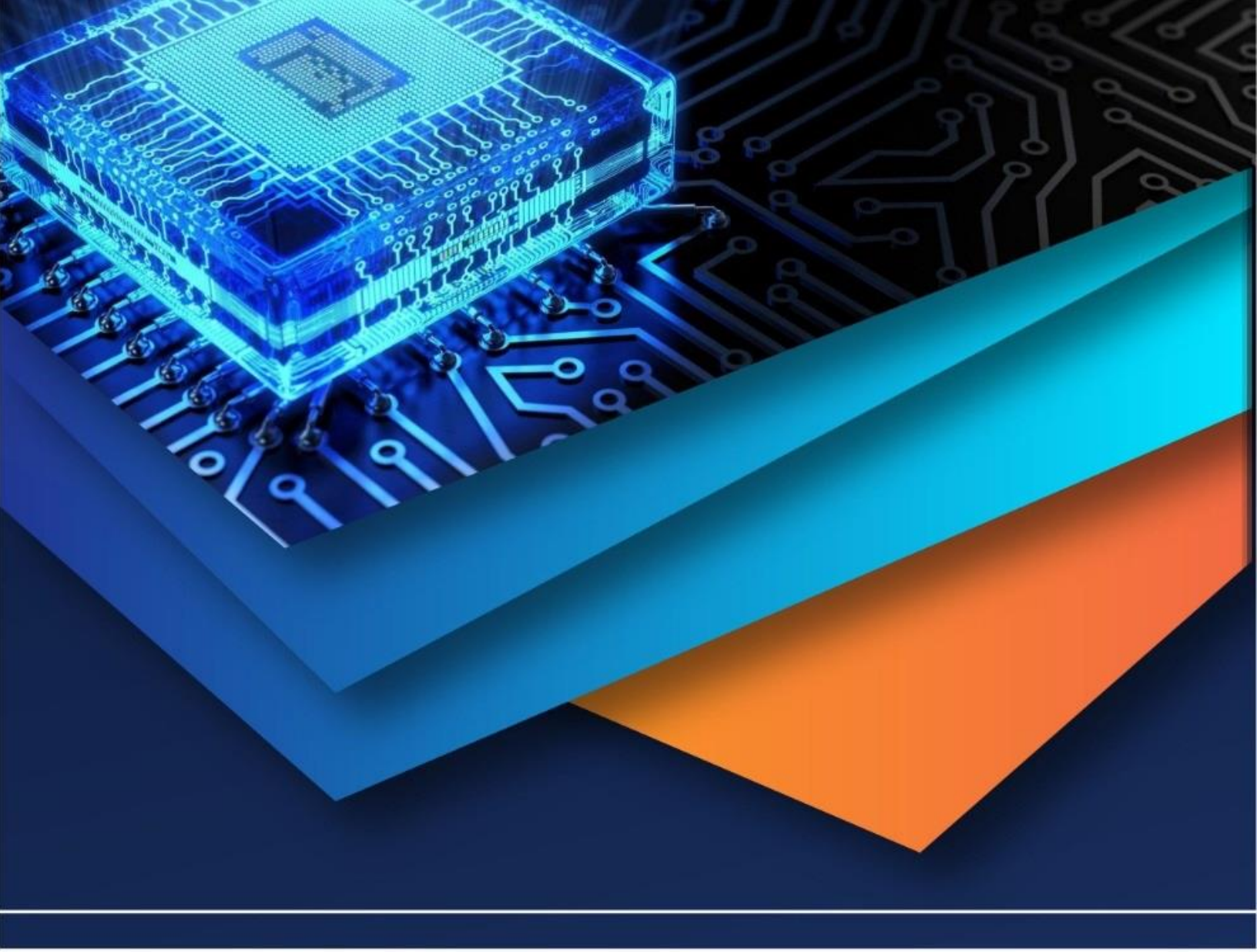
[9] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Comm. Surveys & Tutorials, vol. 8, no. 2, pp. 2-23, Second Quarter 2006.

[10] Mudasser Iqbal , Iqbal Gondal, Laurence Dooley: "An Energy-Aware Dynamic Clustering Algorithm for Load Balancing in Wireless Sensor Networks" 2006.

[11] O. Younis, M. Krunz and S. Ramasubramanian, "Node Clustering in Wireless Sensor Networks: Recent Development and Deployment Challenges," IEEE Networks, May/June-2006, pp.20-25.

[12] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "Wireless Sensor Networks: a survey," Elsevier Science Journal of Computer Networks, vol. 38, 2002, pp. 393-422.

©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)