iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** VI **Month of publication:** June 2016

DOI:

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Increasing Network Lifetime by Using Secure Clustering With Reliable Node Disjoint Multi-path Routing in Wireless Sensor Networks

Pavithra .N .S[1], Dr. G.F. Ali Ahammed2
[1]Dept. of Computer science &Engg, VTU PG Centre, Mysore, Karnataka, INDIA
[2]Associate Professor, Dept. of Computer science &Engg, VTU PG Centre, Mysore, Karnataka, INDIA

Abstract— In order to increase the network latency and resolve the security bottlenecks induced by the camouflaged malicious nodes in Wireless Sensor Networks, the residual energy and trust values are used to form a secured clustering, the network lifetime is increased by using the backup nodes in order to distribute the load among the secured clusters and reliable multi path node disjoint route discovery algorithm is proposed. The simulated experimental results in NS2 platform show that the proposed method can minimize the effect of malicious nodes and improve the network lifetime for the sensor network by balancing the trust values and residual energy of sensor nodes.

Keywords— Wireless Sensor Networks (WSN), Secure Clustering, Network Latency, Reliable Routing With Multiple Node-Disjoint Path, Residual Energy and Node Trust Value.

I. INTRODUCTION

Wireless Sensor Networks are known for their fault tolerance and good sensing coverage. Recently, Wireless Sensor Networks are tremendously being used in various applications like monitoring, detection, process control, data gathering and many more. In spite of all these leads, WSNs are highly susceptible to security ultimatum, energy constraints and impingement by malicious nodes. The camouflaged malicious nodes in the sensor networks can seriously distort the normal functioning of wireless sensor networks. Once the malicious nodes launch the attack, the incursions are hard to identify. Sensory nodes are battery powered which are shielded with a limited energy resource and is one of the exigent demands when it comes to network design consideration. Prolonging the lifetime of sensor networks is quite challenging which requires careful selection of sensor nodes to perform a given task. Recently there has been an extensive ongoing research in the field of reliable routing protocols to provide secure routing and increase the network lifetime. The reliable routing, network latency, secure data aggregation and network scalability are the important issues in wireless sensor networks.

The contribution of this paper is to give a secure load balanced node clustering using trust values of nodes, secondary backup cluster head nodes and providing reliable node-disjoint multi path route discovering method in the wireless sensor networks. The masked malicious nodes is detected based on behavioral changes of nodes and the network lifetime of the sensor network is increased by balancing the trust values, residual energy and the backup cluster head nodes is used to dispense the load among the clusters.The remainder of this paper is organized as follows. Section II describes the related works. Section III discusses the secured clustering with load balance in WSNs. Section IV will propose reliable node-disjoint multi-path route discovering algorithm. Section V evaluates the simulated experimental results in NS2 platform. Section VI concludes the paper.

II. RELATED WORK

LEACH is the initial and very well accepted concept of clustered routing without embedding security. Sec LEACH provides an efficient solution for secure communication in LEACH with the help of random key pre-distribution and TESLA vanquishes some of the attacks. Again to provide effective solution for secure communication in LEACH, RLEACH has been instigated with improved random key pre-distribution scheme. The secure clustering and multiple disjoint reliable path routing method are proposed in which remarkably reduced the influence of malicious nodes increasing the reliability of transmitting the aggregation results. A robust trust-aware routing framework is designed and implemented for dynamic wireless sensor networks that provide the trustful and energy-efficient scalable route without time synchronization or known geographic information to secure the wireless sensor networks against opponents misdirecting the multi-hop routing. The Minimum Total Transmission Power Routing (MTPR) was

proposed to conserve the total power consumption of nodes in the selected route. The Power-Aware Multi path Routing Protocol (PAMP) in is the augmentation of AODV to conserve the node energy using multi path route by modifying RREQ and RREP packets.

III. SECURE LOAD BALANCED CLUSTERING

The following is the design considering for the secure clustering implementation: It is assumed that N nodes are evenly and randomly distributed in the area of L x W with the base station set at the fixed position. During the initial implementation, it is assumed that there are no malicious nodes and each node executes the neighbor finding protocol. The secret key is distributed in advanced using key management protocol in order to have a secure communication path.

During clustering, the node makes use of DSDV routing protocol for the initial data transmission between the given node and the far most node. After the initial data transmission, the remainder energy of nodes is determined and trust values is computed based on the acknowledgement packets received by nodes during transmission. The table I depict the neighbor table (NT table) of all the nodes which consist of parameter computed after the initial transmission. In the table I, NID represents Node Identification number, T represents the trust value of nodes, State denotes the current state of node whether the node is in active state or idle state and Er is the remainder energy of the node.

After the initial data transmission, the nodes which have received comparatively high acknowledgment packets and have greater energy are declared to be the tentative primary cluster head node. The nodes form the clusters by joining its nearest Cluster head node. The Cluster head node broadcast the head message to its neighbors and then computes the average remainder energy of all other nodes in the region of communication radius of node ni using equation (1)

$$Eavg_i = \sum_{j=1}^{m_i} \frac{Er_j}{m_i} \quad i = 1 \sim N \qquad (1)$$

In equation (1), N is the total number of nodes in WSN, mi is the number of cluster members in a cluster and Er j is the remaining energy of the nodes. The time to declare the secured cluster head node is computed by equation (3)

$$T_r = T(n_i)/(T_H) \qquad (2)$$

$$T_{CH} = \tau_1 \times \left(\frac{E_{avg_i}}{E_{r_i}}\right) + \tau_2 \times (1 - T_r) \qquad (3)$$

In equation (3), T = T1+T2 is the durative time of executing the secure cluster head node selection algorithm, Tr is the ratio of trust value of a given node *T(ni)* to the highest trust value of all nodes *TH* as calculated from equation (2) applied to each cluster designed. If *T CH* is small, selecting the cluster head node will be more reliable. If during the transmission of Head_msg from the cluster head node, the current time is less than the calculated time *T CH*, and if the cluster members have overheard the Head_msg from the tentatively selected cluster head nodes, then that node remains as a valid secured cluster head else the remaining nodes in the clusters broadcast the Head_msg and the one which has the highest received acknowledgement packet is declared as the secured cluster head node. Once the secure cluster head is declared, the nodes join the nearest cluster to them. If *d i* is the distance of a cluster member node with respect to the Cluster head node, and *d avg* is the average distance of all other nodes k, with respect to Cluster head node in a cluster C i , then is given by equation (4)

$$d_{avg} = \sum_{i=1}^{k} \frac{d_i}{k} \quad i = 1 \sim N \qquad (4)$$

If *di* < *d avg* , the cluster member node *ni* is the active cluster member.

Next from the NT table, we choose the next node with comparatively high trust value and remainder energy to be as a backup node that will be exchanged as a secondary Cluster head node for the data transmission for certain period of time in alternate rounds once

the reliable path is chosen using reliable multi-path route discovering algorithm in order to balance the energy consumptions of aggregator node and increase the network scalability.

Algorithm 1 Secure Load Balanced Clustering

Step1: Compute remainder energy after initial random data transmission and trust value T by the acknowledgement packets received during data transmission using NT table as shown in Table I.

Step2: The node with comparatively high trust values and remainder energy are elected as the tentative primary cluster head node and its neighbors are selected as cluster member to form a cluster.

Step3: The tentatively selected cluster head node broadcasts the head message (head_msg) to its neighbor cluster members.

Step4: Compute time TCH using (2) and (3)

Step5: While (during broadcasting of Head message by tentative Cluster head nodes) do

If (current time < T CH) then

If (Head message is overheard from the tentatively selected Cluster Head NT[i]) then

Cluster head selected NT[i] is secured primary Cluster head.

Step6: Else

Cluster member declares itself as Cluster_Head;

Broadcast the Head_msg;

Step7: The node which has the highest acknowledgement packets received during broadcasting is selected as the secured primary Cluster_Head.

Step8: The primary secured Cluster Head node broadcasts the Head_msg to all its near neighbors.

Step9: If (State = Cluster_member) then Send join message to the nearest Cluster_Head ;

Step10: From (4) If (The node with distance d i to the Cluster head node < average distance of all the cluster members to Cluster Head nodes d avg) then

Cluster_member_state = active

Step11: Else

Cluster_member_state = idle

Step12: Among the Clusters formed, nodes are chosen to be the active cluster member for a particular duration of time.

Step13: For each cluster, the cluster member which is in the idle state, the node with comparatively high trust value and residual energy are chosen to be the secondary backup Cluster Head.

IV. RELIABLE DISJOINT MULTI-PATH ROUTE DISCOVERING

After Secured Clustering, if the Source node S has data to be sent to the destination Base station node BS, node S will first send the route request RREQ packet with its node identification NID, RREQ sequence number (SeqNo), source address, destination address and MAC value that is calculated based on the secret key KSD which is shared with source and destination. The confirmation key is shared with the node and corresponding neighbor aggregator nodes. The RREQ is forwarded to the neighbor cluster head nodes and it sends the confirmation key to source node for the successful arrival of the packets. The neighbor node then forwards the packet to the next trustful cluster head node. While during routing, if the intermediate node receives the same copy of RREQ packet from multiple node, then it will discard the packet which was received in the last hop and forwards the RREQ to the next trustful node till the destination is received forming a disjoint multiple path route.

Upon receiving the RREQ packet by the destination node BS, it calculates MAC based on the RREQ message received using the secret key KSD. If the MAC calculated matches to the MAC value sent by source, then it knows that the source is authenticated and

generates the RREP packet. The RREP packet along with destination ID, Source ID, sequence number is sent to its neighbor and back to the source using the route table. Once the reliable path set is obtained, data transmission occurs in the multiple paths with the primary cluster head exchanged with the secondary backup cluster head in the alternate rounds for certain duration of time to balance the load among the clusters and increase the network lifetime.

Algorithm 2 Reliable Disjoint Multipath Route Discovery

Step1: The Cluster_Head generates a route request packet RREQ with Node ID, destination address, source address, RREQ sequence number and computes MAC value with secret key KSD .if it has any data to be transmitted.

Step2: The Cluster_Head broadcasts { RREQ packet , MAC, Node ID, Source address, destination address, SeqNo, Confirmation Key } to its neighbor Cluster_Head nodes { N1,N2… Ni }.

Step3: If the Confirmation key matches , the Ni receives the packet , attaches its ID Ni forwards the packet to the next node which has high trust value.

Step4: If the intermediate node say node G receives the same RREQ packet from neighbor nodes, it will discard the packet received from the last hop node and forwards packet to next trustful nodes { RREQ, MAC, Node ID, source address, destination address, SeqNo, ID Xi, ID G } till destination is reached.

Step5: At the destination, Base Station BS calculates MAC based on the packet received using secret key KSD. If the computed MAC value matches the MAC sent from source, then the destination knows that the received packet is not corrupted during transmission.

Step6: The Base station BS broadcasts { RREP packet , MAC, Node ID, Source address, destination address, SeqNo, Confirmation Key } to its neighbors and finds route back to source using route table.

Step7: Once the disjoint multiple path set is obtained for the given Source and Destination, the data transmission occurs between them only in the path chosen.

Step8: While during data transmission after the reliable path is obtained, the Cluster Head is exchanged with the backup Cluster Head node for certain duration of time in alternate rounds in order to balance the load among the cluster and increase the network lifetime.

Step9: If the primary Cluster Head is dead, then the secondary Cluster Head will continue the operation increasing the network lifetime.

In algorithm 2, if a disguised malicious nodes launch wormhole attack or Sybil attack, then MAC computed at the destination will not be matched and the route will be permanently isolated. The cluster containing the malicious nodes can be detected based on the packets dropped. If there are huge packets dropped in the cluster, then that cluster is considered to have a malicious node.

V. EXPERIMENTAL RESULTS

The proposed algorithm is experimented in Network Simulator NS2 platform on a computer with Intel Core i3-380M Processor 2.53GHz and 3GB RAM running Ubuntu 10.02. The number of sensor nodes is chosen to be 80 which are randomly distributed in 2800 x 2500 square region with the base station fixed at a certain region. The sensor nodes are initially assigned with the energy of 30 Joules and DSDV routing protocol is used. The simulation is carried out for 1000 seconds. Some nodes in the sensor network are randomly selected as the malicious nodes. Once the Sybil attack or Wormhole attack, there will be huge packets dropped. The destination checks for the authentication of the source using secret key KSD shared with source and destination. If the malicious nodes launch attack, the attacker will change the source address to its own address as if it's generated from them and forwards RREQ packets to the destination. At destination, since the MAC computed using secret key KSD is not matched, the destination knows that the path is not safe and the path will be permanently isolated. Also since backup nodes are used for data transmission in the reliable path chosen for the alternate rounds, the load is balanced among the clusters and the network lifetime is increased. Figure 1 shows the selected reliable multi path in NAM window between the source and destination node with two different colors brown and maroon representing two separate paths where data transmission takes place. The remaining path is isolated due to the hidden malicious node in cluster6.

Volume 4 Issue VI, June 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

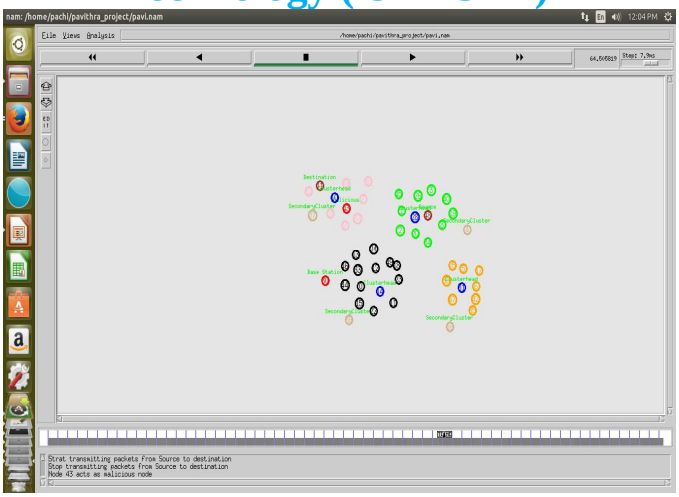


Figure1. NAM window depicting two reliable multiple path source and destination.

Figure 2 shows the cumulative number of packets dropped when Secure Load Balanced Clustering–Reliable Multipath Route Discovery algorithm (SLBC-RMRD) is used and the Simple Route discovery with no local detection (SR) is implemented with 80 nodes and 2 malicious nodes, where the attacker launches attack after the simulation period of 55seconds. In the figure 2, we see that, the cumulative packet loss tend to increase gradually with increase in time since there is no local monitoring and failure in the detection of malicious nodes for simple route discovery. The cumulative packet loss is less when secure load balanced clustering–reliable multipath routing is implemented since it detects malicious nodes and completely isolates the path. The simulation results show that packet delivery ratio in case of SLBC-RMRD is 76.63 % and the packet delivery ratio in simple routing without reliable routing is 68.66%.

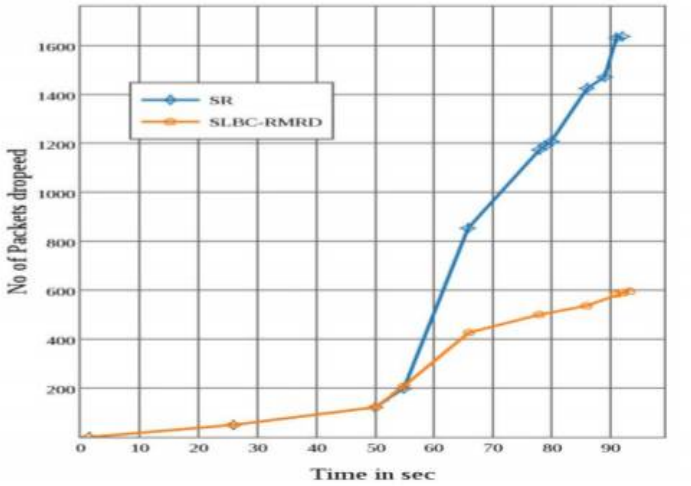


Figure2. Cumulative Number of packet drop for the Simple Routing and Secure Load Balanced Reliable Multipath Route Discovery algorithms.

Figure 3 shows the increase in the network lifetime of proposed Secure Load Balanced Clustering-Reliable Multipath Routing using backup Cluster Head nodes(SLBC-RMRD) than the Secure Clustering_Reliable Multipath Routing without using backup cluster Head nodes(SC-RMRD).The network is said to be expired if 60% of nodes have 0J of energy. The number of data transmission rounds taken till the network switched to dead is more in case of secure balanced_reliable multipath routing without using backup Cluster Head nodes. From the figure 3 we see that approximately 45nodes have lost all energy,0 Joules at the approximate time 857.6 seconds in SC-RMRD and in case of SLBC-RMRD approximately 45 nodes have 0 Joules energy at the simulation period of 916.9 seconds thus the network lifetime is increased in SLBC-RMRD.

Volume 4 Issue VI, June 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

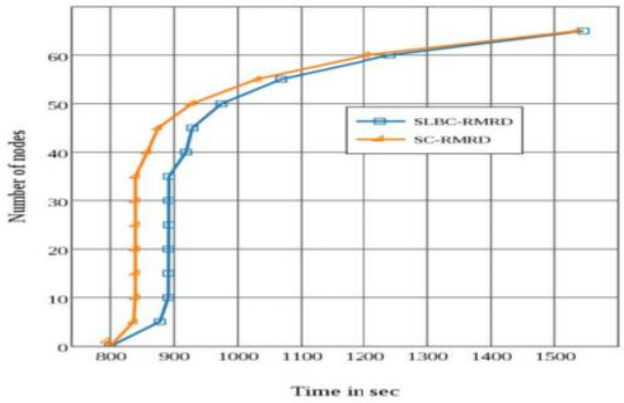


Figure3. Network latency depicted with total number of expired nodes for SC—RMRD and SLBC- RMRD.

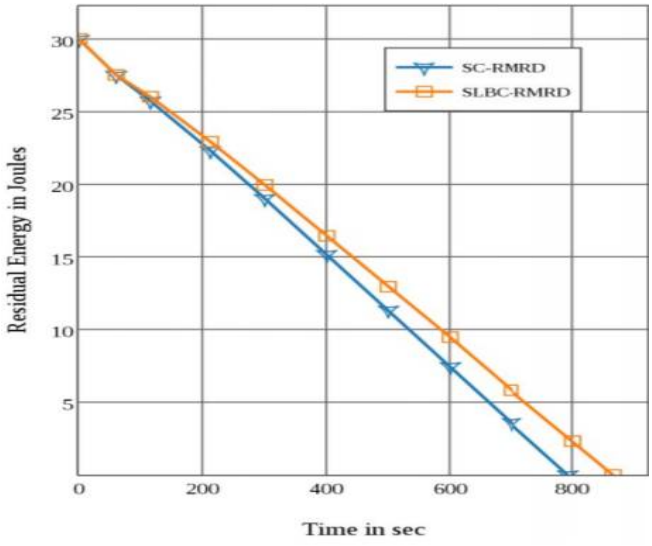


Figure4. Network latency of an individual cluster head node using SC—RMRD and SLBC- RMRD.

Figure 4 shows the network lifetime of an individual secure cluster head node implemented using both the algorithms. The cluster head node has 0 Joule of energy at the simulation period of 793.16 seconds in case of SC—RMRD and the Cluster head has 0 Joules of energy at the simulation period of 864.9 seconds in SLBC-RMRD. The network lifetime of a node is increased in case of SLBC-RMRD algorithm. The lifetime of network in secure clustering-reliable multipath routing without using backup Cluster Head nodes is less as the whole load is induced in the single aggregator Cluster Head node. Also in case of cluster head failure due to the energy depletion, other cluster head continues to work without affecting the topology of the sensor network thus maximizing the network lifetime.

VI. CONCLUSION AND FUTURE WORK

In this paper, the detection of malicious nodes in wireless sensor networks and energy utilization has been done by secured clustering with load balance and reliable multi path node-disjoint routing technique. The basic idea is to balance the remainder energy and trust value of node to select secured primary and secondary backup cluster head nodes to balance the load among the clusters which increase the network lifetime. Also the security is embedded by analyzing the behavior of nodes in a cluster. If a node dropped all the information, which implies that a node has been comprised or is malicious. In proposed algorithm energy utilization is distributed among the cluster heads which makes it work longer than the cluster with single cluster head . Also in case of primary cluster head failure due to energy depletion, secondary cluster head continues to work without affecting the topology of the sensor network thus maximizing network lifetime.

In future, To increase the network lifetime efficiently, we can implement the network in such a way that instead of using secondary

cluster head,provide very high energy for primary cluster head itself. This leads to resolve the confusion among cluster heads. To provide network security, the application has to develop the network it should not experience the malicious attack. if any one of the node is ready for compromise with malicious attack based on the probability the node will be blocked.

REFERENCES

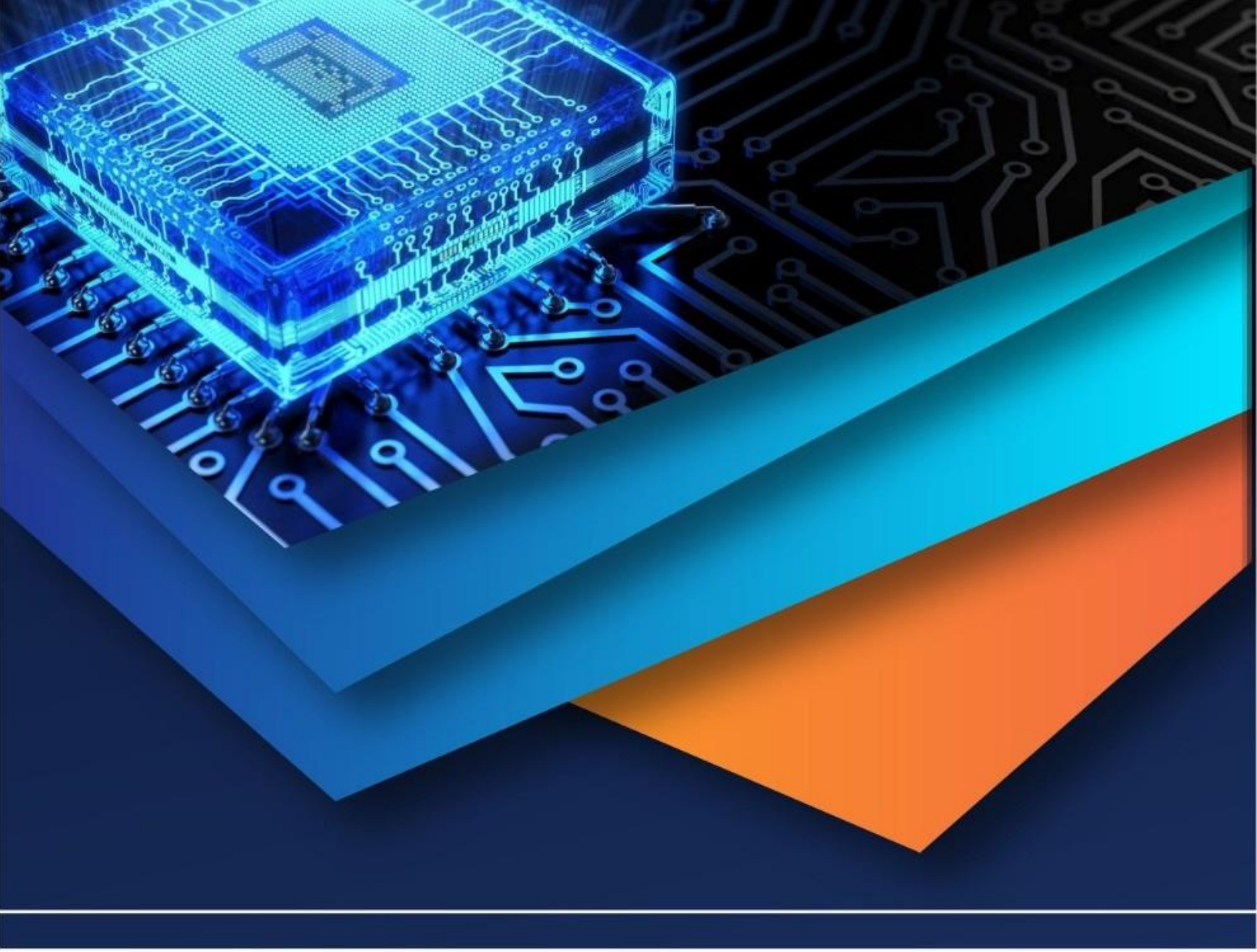
[1] Sudip Misra, P. Venkata Krishna and Kiran Isaac Abraham, "A simple learning automata-based solution for intrusion detection in wireless sensor networks" Wireless Communicattions and Mobile Computing ,vol.11, no. 3, pp. 426–441, March 2011.

[2] Haiguang Chen, Huafeng Wu, Xi Zhou, Chuanshan Gao, "Reputation-based Trust in Wireless Sensor Network" in Proceeding of International Conference on Multimedia and Ubiquitous Engineering (MUE'07), pp.603-607, April 2007

[3] L. B. Oliveira, A. Ferreira, M. A. Vilaa, H. C. Wong, M. Bern, R. Dahab,and A. A. F. Loureiro. Secleach , "Secleach-on the security of clustered sensor networks 87(12) pp. 2882–2895, December 2007.Dgdg

[4] K. Zhang, C. Wang, and C. Wang, "A secure routing protocol for cluster-based wireless sensor networks using group key management" in proceedings of 4th IEEE International conference on Wireless Communications, Networking and Mobile Computing (WiCOM'08) , pages 1–5, October 2008

[5] Cheng Zhong,Yinghong Mo,Jing Zhao, Cong Lin, Xiangyan Lu "Secure Clustering and Reliable Multi-path Route Discovering in Wireless Sensor Networks", in proceedings of Sixth International Symposium on Parallel Architecture, Algorithms and Programming(PAAP), pp. 130-134, 2014.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY