iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 1 **Issue:** V **Month of publication:** December 2013

DOI:

www.ijraset.com

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

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Best Path Routing Algorithm for IDS

Tomar Kuldeep, Arya Richa

Computer Science and Engineering Department
NGF college of Engineering & Technology, Palwal

ABSTRACT

In networking there can be any type of security compromise.IDS detects such type of security threat. Information is transferred from one point to another point across the network. There may be various paths between source and destination. But providing best routing path is very important in network.This paper uses different routing algorithms. These efficient algorithms provide good performance for transferring of data over the network.

Keywords: network, performance, routers, metrices, hop.

INTRODUCTION

Intrusion can be defined as any set of actions that threatens the integrity, availability, or confidentiality of a network or data residing on that network.
Intrusion may be of any type-

- DOS(denial of services) attempts to starve a host of resources which are needed to function correctly.
- Worms and viruses replicating on other files and cause them to improper functioning.
- Hacking, theft, alteration of data
- Or any other type which try to compromise the security of the system.

A system that performs automated intrusion detection is called an Intrusion Detection System (IDS). Whenever any threat occur ,IDS detect that threat and report to the system administrator.

How IDS detect intrusion-

1. Monitoring and analyzing traffic(user and program activities)
2. Identify abnormal activities
3. Raising alarm

IDS Architecture

1. Sensors(agent)→ IDS agent collect all the data and forward it to the analyzer.
2. Analyzer → It receives information from sensor or any other analyzer and then detect all the data if any intrusion has occurred.
3. User Interface → User interface enable user to view output from the system.

IDS detects intrusive behavior in an automated fashion. It monitor activities across NIDS and HIDS and then analyze (detect) activities for sign of intrusion.
It uses two approaches for detection-
1.Anomaly based→ It monitors normal network activities like what sort of bandwidth, protocols are used.

2. Signature based→ It monitors packets in the network and compare them with the pre-determined pattern known as signature.

As it detects any sign of intrusion, it raises alarm to indicate that any abnormal activity has occurred in the system and it also respose to intrusion by blocking specific actions performed by abnormal activities.

IDS can be host-based, if it monitors system calls or logs, or network-based if it monitors the flow of network packets.

In case of network based IDS, basically we give attention on the network .It contains flaw of information in the form of packets. These packets move from one point to another point in order to provide data across the network.

And it can be hybrid type which is the combination of both host and network based IDS.

Routing refers to the process of moving packets of information across a network. Router perform two functions. These tasks are :- deciding the paths for data transfer and sending the packets on these paths. The routing algorithm decides the output line to transfer the incoming packets. The routing algorithms are based on the routing protocol that uses metrics to assess whether a particular path is the optimal path available for transfer of the data packets. The metrics used for evaluating the paths are bandwidth, delay and reliability. The routing algorithms use these protocols to determine an optimal path from the source to the destination. The routing tables maintain all the information related to routing. There are various routing algorithms and depending on these routing algorithms, the information stored in the routing table varies. Every router has its own routing table and it fills this table with the required information to calculate the optimal path between the source router and the destination. It forward packets of data through network.

A routing protocol is a protocol that specifies how routers communicate with each other, gaining information that enables them to select routes between any two nodes on a computer network, the choice of the route being done by routing algorithms. Each router has *a priori* knowledge only of networks attached to it directly. A routing protocol shares this information first among immediate neighbors, and then throughout the network. This way, routers gain knowledge of the topology of the network. The major job of the routing protocol is to provide the information needed by the routing algorithm to compute its decisions.

ROUTING METRIC

Routing algorithms have used many different metrics to determine the best route. Routing algorithms can base route selection on multiple metrics, combining them in a single (hybrid) metric. All the following metrics have been used:

- Path length
- Reliability
- Delay
- Bandwidth
- Load

ROUTING SCHEME

A set of Routing Protocols→

Allows end systems and intermediate systems to collect and distribute information necessary to determine routes.

Routing Table→

Table containing all routing relevant connectivity information.

Routing Algorithms→

Uses information in routing information base (table) to derive routes between end systems.

ROUTING PROTOCOLS

- IGRP (Interior Gateway Routing Protocol) is a distance vector protocol which uses five criteria to determine the best path: the link's speed, delay, packet size, loading and reliability.
- BGP (Border Gateway Protocol) is a distance vector protocol used to exchange routing information between Internet service providers (ISP). Routers using BGP, exchange routing information using TCP connection

It is also used to communicate between two autonomous system.

- RIP (Routing Infrmation Protocol) is a distance vector protocol used to provide information about routing.
- IS_IS (Intermediate system to intern\mediate system) is a link state protocol used to communicate between intermediate systems.
- OSPF (Open shortest path first) is a link-state routing protocol that calls for the sending of link-state advertisements to all other routers within the same hierarchical area.

ROUTING ALGORITHMS

In the network different packets move from one point to another point in order to provide the information across the network. So there are different paths by which they can reach from source to their destination. The problem arises to choose such a path with which packet can be transferred with minimum loss, minimum time and no other difficulty. So a router with the help of certain algorithms calculates the best path for the packet to reach the destination. These algorithms are called routing algorithms.

There are various algorithms which are used for routing-

1. Static routing algorithm
2. Dynamic routing algorithm
3. Single path routing algorithm
4. Multiple path routing algorithm
5. Intradomain routing algorithm
6. Interdomain routing algorithm

Two basic routing algorithms are,

1.Distance-vectoralgorithm.

2. Link state routing algorithm.

1. Distance Vector Algorithm→

It is a type of dynamic algorithm. It uses RIP, IGRP and BGP protocols for routing. As from the name suggests it uses distance and direction to find the best path to reach the destination. The distance here is the number of hops a packet crosses to reach the destination. Each hop refers to a router across the path. The word vector refers to the direction of the packet to reach the destination. Each router knows the id of every other router in the network. Each router maintains a vector with an entry for every destination that contains:

- The cost to reach the destination from this router.
- The direct link that is on that least cost path.

Each router, periodically sends its vector to his direct neighbours. Upon receiving a vector a router updates the local vector based on the direct link's cost and the received vector.

It tells neighbours when it knows about whole the network. It has more knowledge only about neighbours as it interact only with its neighbours.

. Working of this distance vector algorithm can be explained in three steps. The steps are as follows→

Step 1: In this algorithm, router maintains only one routing table in which neighbours entries are taken. Information about the whole network will be sent periodically to all the neighbouring routers connected to it. In this way every router updates the information in its routing table.

Step 2: All the information collected by a single router about the whole network will be sent only to its neighbours and not to all

other routers in the routing table. If there is any change in the hop count or disabled paths it will updated only to its neighbours which in turn after a period passes to its neighbours.
Step 3: The above explained sharing of information will take place in a period of 30 seconds. If
any change in the network occur like if a network fails or additionally a router is added to the network, the changed information will be updated to the neighbouring nodes only after that time period.

Distance vector algorithms use the Bellman-Ford algorithm. This approach assigns a number, the cost, to each of the links between each node in the network. Nodes will send information from point A to point B via the path that results in the lowest total cost (i.e. the sum of the costs of the links between the nodes used). Negative weights also may be taken. When a node first starts, it only knows of its immediate neighbours, and the direct cost involved in reaching them. Each node, on a regular basis, sends to each neighbour its own current idea of the total cost to get to all the destinations it knows of. The neighbouring node examine this information, and compare it to what they already 'know'; anything which represents an improvement on what they already have, they insert in their own routing table. Over time, all the nodes in the network will discover the best next hop for all destinations, and the best total cost.

Routing table maintains the list of destinations, the total cost to each, and the next hop to send. When one of the nodes involved goes down, those nodes which used it as their next hop for certain destinations discard those entries, and create new routing-table information. They then pass this information to all adjacent nodes, which then repeat the process. Eventually all the nodes in the network receive the updated information, and will then discover new paths to all the destinations which they can still reach.

BELLMAN-FORD EQUATION-

$d_x(y)$:= cost of least-cost path from x to y

$d_x(y) = \min \{c(x,v) + d_v(y) \}$

where min is taken over all neighbors v of x

2.Link state routing algorithm:

It is also a type of dynamic algorithm. It uses OSPF and IS-IS protocols for routing. In this algorithm, each node uses as its fundamental data a map of the network in the form of a graph. To produce this, each node floods the entire network with information about what other nodes it can connect to, and each node then independently assembles this information into a map. Every node tells its neighbour node what it knows about a ll the network.

Each router uses that map to determine the least- cost path from itself to every other node. Router then construct the routing table, which specifies the best next hop to get from the current node to any other node. It uses three tables for the calculation of the routing table entries.
First table contains information about the neighbours.
Second table contain information about the whole topology.
Third table is the actual table which calculates the best path for the given node.

Link-state algorithms use Dijkstra algorithm. It finds the shortest path from that node to the destination. First it calculates its distance from the neighbours and pass this information across the network. Then it uses the shortest path to its neighbour and reach to the destination.

It has several advantages over distance vector algorithm. Some of them includes, its faster convergence time, ability to handle very large networks, reliable path prediction. It uses link state advertisements to find the information about the router.

Working of this distance vector algorithm can be explained in three steps. The steps are as follows,

Step 1: This algorithm uses link state packets or advertisements to collect the information about the neighbouring routers. Only links that are connected directly are considered as neighbours.

Step 2: It sends information to all the routers in the network. In this algorithm totally three tables are maintained. One has

information about neighbours, second has information about the entire topology and third is the actual routing table.

Step 3: In this algorithm there is no periodic updates involved. A router in the network will send updates to all the routers and only if there is a change in the network. That is why it is called as event triggered updates. This event triggered updates will help the router to find its path immediately without any errors. This algorithm uses is-is and ospf protocol

Best Path Algorithm

As far as we have studied so many algorithms for routing, all the algorithms have their own advantages and some disadvantages also. So the main focus of this algorithm is to choose a path which is best from all aspects. Here best path means obviously a path which is best suited for messages so that they can reach from source to their destination. Such a path will always work.

In term of distance, Best path can be assumed as minimum path to reach packet from source to destination. Because at smallest path, packet will reach in minimum time. So there is no problem of time consuming. On the other hand, such a path will be free from packet losses, delay & any other transmission problem. Because if we choose minimum path, that will be taken as best path & this algorithm is known as best path algorithm.

How to calculate minimum path using best path algorithm----

M(i,k) = min [M(i,j) + M(j,k)]

This formula states that the best path between two networks (M(i,k)) can be found by finding the lowest (min) value of paths between all network points. Let's look again at the routing information . Plugging this information into the formula, we see that the route from A to B to C is still the best path:

5(A,C) = min[2(A,B) + 3(B,C)]

Whereas the formula for the direct route A to C looks like this:

6(A,C) = min[6(A,C)]

Where AB = 2, BC = 3 and AC = 6

For a given source vertex (node) in the graph, the algorithm finds the path with lowest cost (i.e. the shortest path) between that vertex and every other vertex. It can also be used for finding costs of shortest path from a single vertex to a single destination vertex by stopping the algorithm once the shortest path to the destination vertex has been determined. For example, if the vertices of the graph represent cities and edge path costs represent driving distances between pairs of cities connected by a direct road, This algorithm can be used to find the shortest route between one city and all other cities.

ALGORITHM

Pi: path from i

Vn : vector set of n nodes

Cpath : given path

On receive vector link V(i,k)

Vi← 0

1 . [T].i = [T].i + v[d].i

//insertion in routing table[T]i

2. for each row in [T]i

do

if Cpath (j) = min [d],i.j

// updation in routing table

Vi ← Vi union (j. Cpath(j))

3. if Vi ! = 0

Send Vi to all neighbours

4.On get failure (i.k)

Delete column k in Di and

execute 2 & 3

5.On receive recover(i.k.dik)

Insert column k in Di

Vk = {k, dik }

is received on link (i ,k)

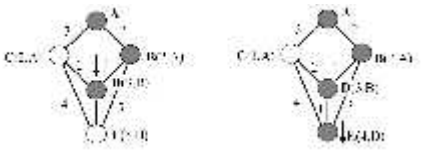
6. Copy whole routing table into Vi and send to k

EXPLANATION

In step (1), the routing table is checked for paths to the given k , where k is given destination. The newly changed distances are computed.

Step (2) makes the necessary changes to the routing table and the preferred successor.

Step (3) assures the proper updates are sent to the neighbouring node. When a failure notice is received , the entry is removed from the routing table, that means that nodes are removed and then changes are broadcast to the network. Similarly when a new node makes its presence known, the entry is added to the table, calculation are completed to determine if this new node will aid in any shortest path and then , the new updates will be broadcast to the neighbours

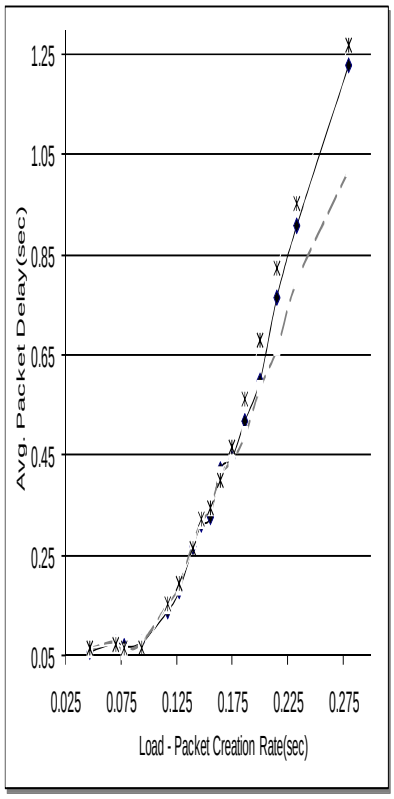


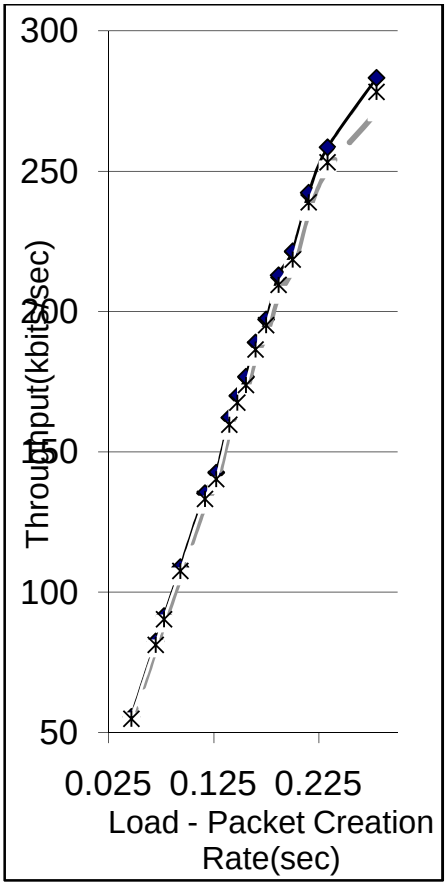
For the given figure, best path from A to E is from A to B, B to D and D to E. So best path algorithm chooses best path which is minimum in terms of cost.

PERFORMANCE PARAMETERS

Average packet delay: It is the average delay a packet experiences while being routed from source to destination.

Average throughput per packet: It is the average number of packets being forwarded by a node for the duration of the simulation.





IMPLEMENTATION

The implementation of best path algorithm is based on a min-priority queue implemented by a Fibonacci heap and running in $O(|E| + |V| \log |V|)$

An upper bound of the running time of this algorithm on a graph with edges E and vertices V can be expressed as a function of $|E|$ and $|V|$ using big-O notation.

For any implementation of vertex set Q the running time is in $O(|E| \cdot dk_Q + |V| \cdot em_Q)$, where dk_Q and em_Q are times needed to perform decrease key and extract minimum operations in set Q, respectively.

The simplest implementation of the this algorithm stores vertices of set Q in an ordinary linked list or array, and extract minimum from Q is simply a linear search through all vertices in Q. In this case, the running time is $O(|E| + |V|^2) = O(|V|^2)$.

For sparse graphs, that is, graphs with far fewer than $O(|V|^2)$ edges, this algorithm can be implemented more efficiently by storing the graph in the form of adjacency lists and using a binary heap, pairing heap, or Fibonacci heap as a priority queue to implement extracting minimum efficiently. With a binary heap, the algorithm requires $\Theta((|E| + |V|) \log |V|)$ time (which is dominated by $\Theta(|E| log |V|)$, assuming the graph is connected).

Note that for directed acyclic graphs, it is possible to find shortest paths from a given starting vertex in linear time, by processing the vertices in a topological order, and calculating the path length for each vertex to be the minimum length obtained via any of its incoming edges.

CONCLUSION

Networking measurely deals with transmission of data from one place to other place. This paper gives idea for using best path algorithm by implementation of different steps for finding efficient routing path. which give flexibility and reliability to data to reach its destination.

Best routing path not only means reaching data in minimum time. But it also reduces packet delay, faster access to destination and minimum cost. This clearly illustrates the usefulness of routing algorithms for data transmission.

The comparative study also reveals topics for further research. For example, there is need for such routing algorithm which gives highly effective performance.

REFERENCES

1. BROADCASTING INTERNET DATAGRAMS IN THE PRESENCE OF SUBNETS, RFC 922, Jeffrey Mogul, October 1984

2. Medhi, Deepankar and Ramasamy, Karthikeyan (2007). *Network Routing: Algorithms, Protocols, and Architectures*. Morgan Kaufmann. ISBN 0-12-088588-3.

3. Huitema, Christian (2000). *Routing in the Internet, Second Ed.*. Prentice-Hall. ISBN 0-321-22735-2.

4.Neil Spring, Ratul Mahajan, and Thomas Anderson. Quantifying the Causes of Path Inflation. Proc. SIGCOMM 2003.

5.Zhan, F. Benjamin; Noon, Charles E. (February 1998). "Shortest Path Algorithms: An Evaluation Using Real Road Networks". *Transportation Science* 32 (1): 65–73. doi:10.1287/trsc.32.1.65.

6. Leiserson, Charles E.; Rivest, Ronald L.; Stein, Clifford (2001). ". *Introduction to Algorithms* (Second ed.). MIT Press and McGraw-Hill. pp. 595–601. ISBN 0-262-03293-.

7 .Fortz,B,J,Rexford,M.Thorup,Traffic Engineering with Traditional IP routing protocols.IEEE Communicaion magazine,2002.

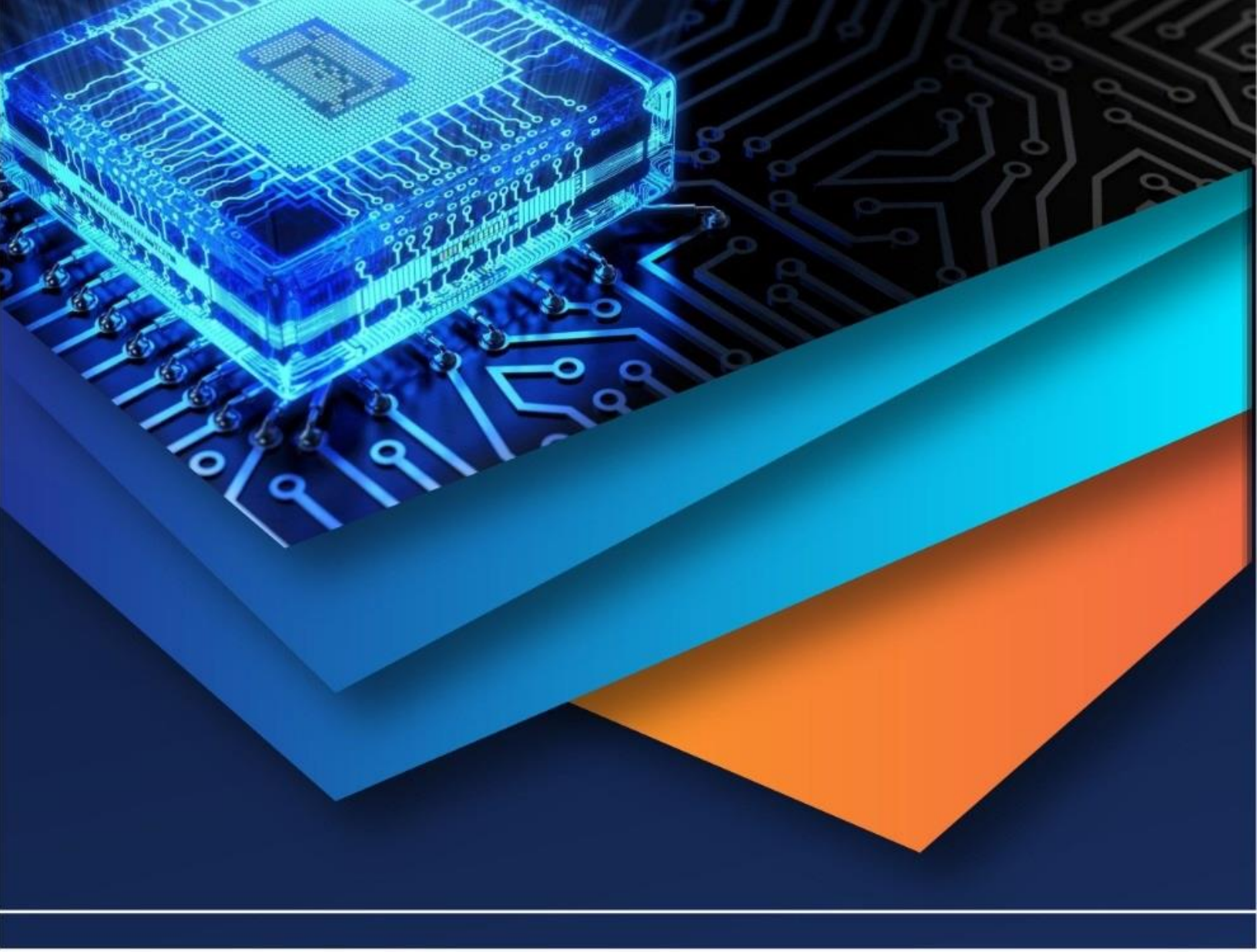
8 .M. Christiansen,M, K. Jeffay, D. Ott, F. D. Smith, Tuning red for web traffic IEEE/ACM Transactions. On networking Vol. 9 No. 3(june 2001)

9 .Zaumen, W.T. Aceves, J.J., Dynamics of distributed shortest path Routing Algorithms. ACM Press.1991

10 .Ahuja, R.K. Mehihorn,K.Orlin J,Tarzan R,faster algorithm for the shortest path problem, Journal of the association fr computing Machinery,vol.37.no.2.1990

11 .Cornien, T.H. Leiserson, C.E.Rivest, R.L. and Stein C. Introduction to Algorithms. Mcgraw Hills . MIT Press.2002.Cambridge.

12. A.Sundaram, “An Introduction to Intrusion system,” ACM Crossroads Students Magazine.1996



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY