iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** VII **Month of publication:** July 2016

DOI:

www.ijraset.com

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

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

Various Attacks Including JellyFish Attack Along With Security Issues In Manet

Devesh Tedia[1], Umesh kumar Lilhore[2]
[1,2]*Department of Computer Science and Engineering*
NIIST, Bhopal, INDIA

Abstract— The MANET which is termed as Mobile Adhoc network works like a wireless network with unrestricted mobility and without any infrastructure. To design a new security mechanism for MANET various attack variations as well as their characteristics must be known. This paper studies distinct kinds of attacks namely - Data traffic attacks, Jelly Fish Attacks, Jelly Fish recorder Attack, Black Hole Attack, Gray Hole. The paper study mainly focuses on the jellyfish attack and its type. The paper also brief various techniques developed to detect and prevent from jellyfish attack.
Keywords: MANET, Attack, Security, Jelly Fish

I. INTRODUCTION

In the Ad Hoc networks, few characteristics exists that certainly enhances the exposure of this network [1]–
Vigorous Topology
Scattered Operation
Resource Limitations
Most of the characteristics are specially utilize to categorize the attacks in such kind of networks. It doesn't not receive the entire threats that comes under the category of security and which are faced in wired and wireless networks. As well as, it initiates the uniqueness of security attacks itself [2]. As people will be encouraged to use a secured network, it is important to provide MANET with reliable security mechanisms if individuals want to see this exciting technology become widely used in a next few years. To secure the mobile adhoc networks, its is really significant to study the variety of attacks that might be related to such networks but do this thing before the security measures. With the knowledge of some common attack issues, researchers know very well about the working procedure of such networks that could be threatened by the attackers, and thus might lead to the enhancement of security measures that are more reliable to protect them.
One of the most significant and essential instrument is Routing in the adhoc networks. When people use inadequate and self-doubting mechanisms in routing so, it is capable to worsen the performance of networks. Nevertheless, it is also reduce the networks that are weak to various security attacks.
One of the basic elements in the routing mechanism is the routing communication, that is specifically utilize to launch and keep the connections that is situated in the middle of the network's nodes. The importance of the routing message has made it a main target by the attackers against the adhoc networks is to establish the attacks [3, 4, 5]. For mobile networks in adhoc category, professionals have to consider the dissimilarities of attacks and characteristics as well in the mechanism of designing security.
The major issue in MANETs is security because the routing protocol consist a break that defines the level of security. The main reason behind that, protocols doesn't have any kind of defense mechanism which is inbuilt to handle the attacks. Hence, such kind of networks frequently face issues from security attacks due to the characteristics – open medium, altering topology which is dynamic, deficiency in central management and unclear mechanism of defense. Due to the casual movement of nodes, the topology alters frequently and nonstop, the spiteful nodes can link the network that reduces its performance. Hence, this is a requirement that works like an alarm bell to read about the distinct types of attacks on protocols of MANET.
As there are several attacks that are not regularly follow the rules and regulations of protocols. But, the jellyfish attackers are good due to their continuously follow the complete set of rules. The actual power of this attack is the acceptance along with the entire data and control plane protocols. This is the main cause of detecting such type of attack seems difficult.
When the attacker of jellyfish reorder is doing restructuring the packets which are already sent from start to end so analyzing the performance level of ZRP protocol is significant. Then, the reordering process finishes and if the complete data get at destination are clubbed, after that the garbled data is produced. It is able to degrade the Good put to a definite level. Therefore, this paper describes the recreation effect that is calculated to govern the routine of ZRP protocol. This is done by the Jellyfish Reorder attacks by

utilizing the two things –
Good put
End to End Delay [6]

II. SECURITY ISSUES

One of the important concerns to secure the network is various problems that are still unsolved. The adhoc networks are weak to attacks due to many reasons; amongst them is lack of secure boundaries, threats from compromised nodes within the network, lack of centralized management facility, restricted power supply, scalability [7]. Mobile Adhoc Systems have various flaws which make it more vulnerable to attacks [8].

A. Non Secure Boundaries

The wireless medium does not have proper boundaries outside of which nodes are known to be unable to receive network frames

B. Compromised Nodes

These networks mobility makes its simple for various nodes like bargained to alter its place. Therefore, it frequently creates the nodes more complex and hard which is unable to track the illegal activities.

C. No Central Management

On the basis of blind mutual trust, the different nodes connected each other and hence, analyzing the attacks and monitor the traffic is little bit clumsy.

D. Problem Of Scalability

In this, nodes can freely move in and out position which make it more scalable and shrinkable.

Following are the key requirements which check whether the security of network is maintained or not.
Availability: Generally, the main aim of DOS attacks and its capability to tolerate the functionalities of networking without any interference is only because of the security threats.

Integrity: During transmission, this process is ensured that the data packet is not manipulated at this time.

Confidentiality: Gives guarantee that particular information is never ever ensures certain information is never revealed to those people or entities that are not authorized.

Authentication: It also gives conformation that the other end of any connection or the creator of data packet is the claimed node.
Non Repudiation: It ensures that the actual source of message has not ability to deny containing the sent message.

III. SOME ATTACKS

Jellyfish attacks work on MANETs that use protocols with congestion control techniques, such as the Transmission Control Protocol (TCP), in the transport layer. JF attacker needs to intrude into forwarding group and then it delays data packets unnecessarily for some quantity earlier dispatching them. Due to JF attack, high end to end delay takes place in the network. So the performance of network (i.e. throughput etc) decreases substantially. Jelly Fish attack is divided into three categories- JF Reorder Attack, JF Periodic Dropping Attack, JF Delay Variance Attack.

A. Jellyfish Reorder Attack

In this attack JF nodes maliciously reorder packets. In this attack, JF deliver all packets, yet after placing them in a re-ordering buffer rather than a First in First out (FIFO) buffer. Consequently, the experts will show that such persistent re-ordering of packets will result in near zero goodput, despite having all transmitted packets delivered. This attack is possible due to well known vulnerability of TCP. Jelly fish attacker uses this vulnerability to record packets. This is possible because of factors such as route changes or the use of multipath routing [9].

B. Data Traffic Attack

This kind of attack compacts in nodes that drops the data packets and is conveying via these nodes. In spite of that, this attack also deals with the delay of those data packets which are forwarded. There are two kinds of attacks in it – first one those who can select

their victim packets to drop and the other one those that drops all the packets with respect to the sender nodes. This mechanism may easily decrease the service quality and enhance the delay time. Due to this, the chances of losing significant data increases. For instance, a wireless link of 100 Mbps acts as a connection of 1 Mbps. In addition, there is a terminated path all around the nodes that are erratic. Few nodes are not able to reach each other in this attack.

C. Black Hole/ SinkHole Attack

They examine the packet delivery ratio of multicast sessions under black hole attacks. A black hole attacker first implement rushing attacks to gain access to the routing mesh, and then later drops the data packets it receives. The processing delay of legitimate nodes is set at 20 ms they investigated various scenarios by varying the number of senders, the number of receivers, the number of attackers, and their positions. In each experiment, they measured the ratio of packet delivery [10]. A malicious node behave just similar as a black hole that drops all the packets conveying via it and act as an energy and matter that evaporates by our world in a hole which is "black". Sometimes, the attacker nodes are connected with the two linked components of such network, after that, it splits the network in to two disconnected components effectively.

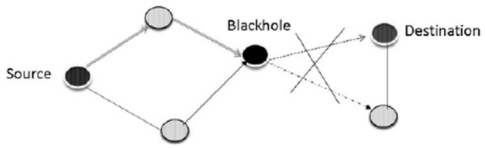


Figure 2: Black-Hole Attack

The node of this attack splits the network into some sections and few strategies to mitigate the problem:
Gathering lots of RREP messages and then hope several terminated paths to the end node move towards the safe route which is found easily.
It maintains a table in every node along with the prior sequencing in the increasing order. Before forwarding he message, each and every node packets will enhances the sequence numbers. The starting node or we can say sender transmits RREQ to its fellow nodes and when it reaches at the end point then it answers along with the RREP and sequence number of last packet. If the middle nodes recognize that it consists a sequence number which is wrong so it know very well that somewhere is went wrong things and that why the numbers sequencing becomes incorrect. [11]

D. JellyFish Periodic Dropping Attack

Periodic dropping is possible because of sarcastically chosen period by the mischievous node. This kind of periodic dropping is possible at relay nodes. Suppose that congestion losses force a node to drop α% of packets. Now consider that the node drops α% of packets periodically then TCPs throughput may be reduced to near zero even for small values.

E. JellyFish Delay Variance Attack

In this type of attack, the spiteful node randomly delays packet without changing the order of the packets. [12]

F. Implementation Of Jelly Fish Attack

In the scenarios of jelly fish attack for all the three protocols i.e. AODV, OLSR and TORA the forwarding rate is taken as 5000 packets per second and in the normal flow scenarios of these protocols the value for forwarding rate is 400000 packets per second. In our work, OPNET 14.0 Modeler is used to analyze the effect of attack namely - jelly fish of routing protocol on Mobile adhoc network. Here, use three protocols AODV, OLSR and TORA. In this paper there are various simulation scenarios to analyze our results. [13]

G. GrayHole Attack

Grey hole attack is a particular type of black hole attack. An enemy acts as a part of the routes of the network such as gets the way and after that, leave the data packets in a selective way [14]. One can't assume the probability of dropping data packets. The attacker node agrees firstly to route packets and then deny to do so, which leads to losing of packets.

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

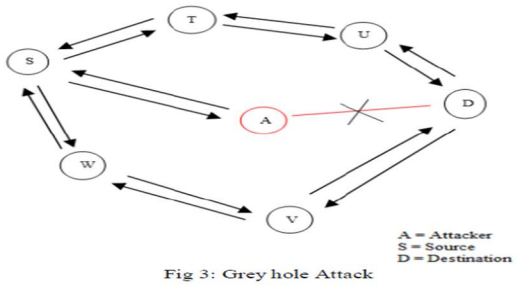


Fig 3: Grey hole Attack

The Gray Hole attack comprises some stages: In the first stage, an attacker node manipulate the AODV which stands "Ad Hoc on Demand Distance Vector" protocol to behave as having a legal route to the destination node, with the aim of disturbing the data packets, even though the route is false. In the second stage, the node that attacks is able to drop the disturbed packets with a positive chance. This type of attack is more complex to find in comparison of black Hole attack in that attacker node beads the obtained data packets with surety.

H. Rushing Attack

In reactive routing protocols, which use duplicate suppression, rushing attack is quite possible. As shown in to the figure.1, consider node X as the source node and node Y as the destination node.M1 and M2 are the two neighboring nodes of destination node Y. In routing activity that uses reactive routing protocol Ad hoc on Demand Distance Vector (AODV).Source node X need to communicate to destination node Y. So, X will broadcasts route request (RREQ) packet. There are multiple paths available via which this RREQ packet reached to node Y. There are two neighboring nodes M1 and M2 passes this RREQ packet finally to the node Y. Now, if H is the malicious node also passes this packet via multiple paths through M1 and M2 speedily then other nodes. It means in all paths RREQ was forwarded through H or in other words H is able to rush its RREQ earlier to destination. Then other legitimate RREQ packets will be ignored as per the protocol rules. So, as a result source node X is unable to find legitimate route with less number of hops.

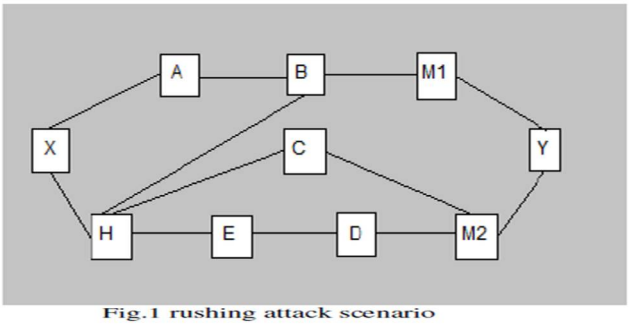


Fig.1 rushing attack scenario

I. Sybil Attack

In MANET – Mobile Ad Hoc Network, the medium for transmission of packets that contains data is air and they are not centralized kind of nodes to manage the network. Thus the routing depends on little exclusive node address. This feature of MANET can be utilized by the attacker for using fraud individualities. It means the enemy can use a identity of legal node or a random identity. This type of attack is called "Sybil attack."

In this attack, it may generate multiple fraud characters. The attacking node can introduce them self as a wide range of nodes rather a single node. These fraud identities are known as Sybil nodes. This attack may induce lots of data packets to be routed in the direction of fraud nodes.

IV. JELLYFISH

The Jellyfish approach is to construct a random graph at the top-of-rack (TOR) switch layer. Each TOR switch I have some number ki of ports, of which it uses ri to connect to other TOR switches, and uses the remaining ki - ri ports for servers. In the simplest case, which consider by default throughout this paper, every switch has the same number of ports and servers [15]

Attackers are always trying to modify messages or generate false messages and thus take down the network's operations which cause DOS (denial of service) in MANETs. In this section the summary introduces "JELLY FISH" Attack.Tremendous progress has been made in order to networks by developing routing protocols which is secure and ensure different security concepts such as

authentication and data integrity. Moreover, IDS (Intrusion Detection) and trust-based systems is now established to prevent MANETs against mischief's like rushing attack, query flood attacks, and selfish behaviors. Yet, most of the techniques in the category of defense are not able to analyze a set of protocol compliant attacks termed as JF attacks.

Jelly fish attack is one of the denials of service attack and also a type of passive attack that is undetectable. It produces delay before the broadcast and response of packets that contains data in the ad hoc network.

Applications such as HTTP, FTP and video conferencing are provided by TCP and UDP. Jelly fish attack disturbs the performance of both protocols. It is same as BF (black hole) attack but the difference is that the attacker nodule leaves all the data packets but jelly fish attacker node produces delay at the time of forwarding packets. Jelly fish attacks are targeted against closed loop flows. TCP has well known vulnerabilities to delay, drop and disorder the packets. Due to this, nodes can change the sequence of the packets also drop some of the data packets. The jelly fish attacker nodes fully obeys protocol rules, hence this attack is called as passive attack [16].

Jelly fish attacks are targeted against closed-loop flows. The goal of jellyfish node is to diminish the good put, which can be achieved by dropping some of packets. When a malicious nodes launches forwarding rejection attacks it also may comply with all routing procedures. The Jellyfish attack is one of those kinds. A malicious node launching Jellyfish attacks may keep active in both route discovering and packet forwarding in order to prevent it from detection and diagnosis, but the malicious node can attack the traffic via itself by reordering packets, dropping packets periodically, or increasing jitters. The Jellyfish attack is especially harmful to TCP traffic in that cooperative nodes can hardly differentiate these attacks from the network congestion. Reference also described in which spiteful nodes can even abuse directional antenna and dynamic power techniques to avoid upstream nodes to detect their misbehaviors of dropping packets.

This attack mainly targets closed-loop flows as such flows respond to network conditions like packet loss and packet delay. It targets TCP's congestion control mechanism. The main goal of the Jellyfish nodes is to reduce the good put of all the flows to near-zero by either reordering the packets or dropping a small fraction of packets. [17] These forwarding mechanisms are variants of Jellyfish attack.

V. LITERATURE REVIEW

The Ad Hoc systems are vulnerable to numerous kinds of attacks because of distinct characteristics like architecture of open system, rigorous source limitations, wireless medium which is shared and at last dynamic topology at higher level. These attacks contain numerous varieties excluding DOS that is the most hard and worst kind of attacks. It cannot be detectable and defendable easily.

The term Jellyfish is a new kind of attack that comes under the denial of service which abuses the end to end control strategy in congestion of TCP – Transmission Control Protocol. It really has an overwhelming effect on the material. The architecture of such attacks for recognized in two things – distributed and cooperative. These things are suitable the requirements of wireless networks that are actively take part in the intrusion detection system. The author intends to build an algorithm which is able to analyze the jellyfish attack on various nodes whether it is at single node and deployed efficiently at all the set of nodes in the network/ systems. They also propose the novel metric which can easily recognize the reorder attack of Jellyfish and based on its density that able to build the metric [18].

Due to this attack, high end- to- end delay is introduced in the network resulting in low performance (i.e. throughput).In this paper the effect of JF Delay Variance attack on MANET using AODV as a routing protocol has been calculated and the performance analysis is done with respect to some network parameters like throughput, end- to- end delay etc. using OPNET modeler. It is observed that MANET is resilient up to 10% of Jelly Fish (JF) attackers. They do not make any hard impact on the performance of network. For attackers above 10% and below 20% performance is affected with an average rate but for 20% or above 20% performance of network becomes worse. [19] Due to the rapidly increases in wireless communication, it arises the distinct kinds of network such as MANETs (Mobile Ad Hoc Networks), WSN (wireless sensor networks) and various other that belongs to this attack. The ad hoc networks are defenseless to plenty of attacks and threats as well because of the characteristics that are unique and effective. These features are act as a non-static topology, visual medium which is mutual, scattered operations and so on. These attacks are seriously affect the working of Mobile Ad Hoc Networks. The Denial of Service is the most common attack that affects the entire set of systems in MANETs. The name Jellyfish is recently earned due to the scenario attack in these kinds of networks. [20]

The experience of industry specifies the capability to increment the data centers which is expandable and is important. Hence, the high bandwidth network that exists and its designs contain inflexible structure. This structure interrupts the network along with the

expansion of enhancement. It presents a high capacity network that interlinked via accepting a topology which is a random graph in Jellyfish. The expansion is a natural process which increments step by step. Unexpectedly, Jellyfish is cost-effective as compared to fat-tree which supports as thousands of servers approx. 1/4rth part complete set of capacity utilizing the similar devices at various nodes and the benefits of scale improving nodes. It also allows a brilliant scale of flexibility in developing networks along with the distinct degrees of subscription which is over-weighted. Hence, the unstructured design of Jellyfish carries latest challenges in the term of routing, physical design and wiring as well. The author explains to resolve the numerous tasks which are discussed about and their assessment suggests that Jellyfish which is easily deployed in the data centers of this era. [15]

VI. CONCLUSION

This paper reviews various attacks in MANET. The main focus of the paper is on the jellyfish attack and its types. The paper also discusses various works done to detect and prevent the jellyfish attack MANET. In future, a technique can be developed to handle more than one jellyfish attack at one time. This paper gives review about the most recent establish attack in wireless networks and is not easy to detect the TCP and other routing protocols. Strong novel mechanism is the need of hour to develop in order to overcome this attack in the network. It will be using Genetic Algorithm as technique to combat the attack and optimize the network and provides defense to Mobile Ad Hoc Networks against this technique.

REFERENCES

[1] International Journal of Engineering, Applied and Management Sciences Paradigms, Vol. 24, Issue 01, “A Review on Jellyfish Attack in MANET”, May 2015.

[2] T. Karygiannis and L. Owens, “Wireless Network Security, 802.11, Bluetooth and Handheld Devices,” NIST Publication, p. 800(48), November 2002.

[3] H. Li, Z. Chen and X. Qin, “Secure Routing in Wired Networks and Wireless Ad Hoc Networks,” Univ. of Kentucky, Department of Computer Science, Termpaper, 2003.

[4] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks," in Proc. of 2002 IEEE International Conference on Network Protocols (ICNP), pp. 778-89,Nov. 12-15, 2002.

[5] Kristoffer Karlsson IT3, Billy HoIT3,Ad hoc networks: Overview, applications and routing issues, Chalmers University of Technology.

[6] International Journal of Computer Applications (0975 – 8887) Volume 109 – No. 9, January 2015, “ Analysis of Jellyfish Reorder Attack on ZRP”.

[7] Aad and J.P. Hubaux, E.W. Knightly, “Impact of Denial of Service Attacks on Ad Hoc Networks”, IEEE/ACM Transactions on Netwroking,vol.16,pp.791-802,Aug.2008.

[8] Kaur Manjot, Nayyar Anand “A Comprehensive Review of Mobile Adhoc Networks (MANETS)” in International Journal of Emerging Trends & Technology in Computer Science (ISSN2278-6856), Volume 2, Issue 6, November - December 2013.

[9] Mr. Hepikumar r. Khirasariya, “Simulation study of jellyfish attack in manet (mobile ad hoc network) using AODV routing protocol”, journal of information, knowledge and research incomputer engineering, issn: 0975 – 6760| nov 12 to oct 13 | volume – 02, issue – 02.

[10] Nguyen, Hoang Lan, and Uyen Trang Nguyen. “A study of different types of attacks on multicast in mobile ad hoc networks." Ad Hoc Networks 6, no. 1 (2008): 32-46.

[11] Himadri Nath Saha & Debika Bhattacharjee “Different types of attacks in Mobile ADHOC Network: Prevention and mitigation techniques”.

[12] International Journal of Computer Trends and Technology (IJCTT) – volume 15 number 1 – Sep 2014, “Simulation of Jelly Fish Periodic Attack in Mobile Ad hoc Networks”.

[13] IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 5, July 2014, “COMPARISON OF AODV, OLSR, AND TORA IN MANET UNDER JELLY FISH ATTACK”.

[14] Nital Mistry, Devesh C. Jinwala and Mukesh Zaveri, “Improving AODV Protocol against Blackhole Attacks”, International Multiconference of Engineers and Computer Scientists 2010, vol. 2, March 2010.

[15] Ankit Singla†_, Chi-Yao Hong†_, Lucian Popa], P. Brighten Godfrey University of Illinois at Urbana–Champaign, “Jellyfish: Networking Data Centers Randomly”..

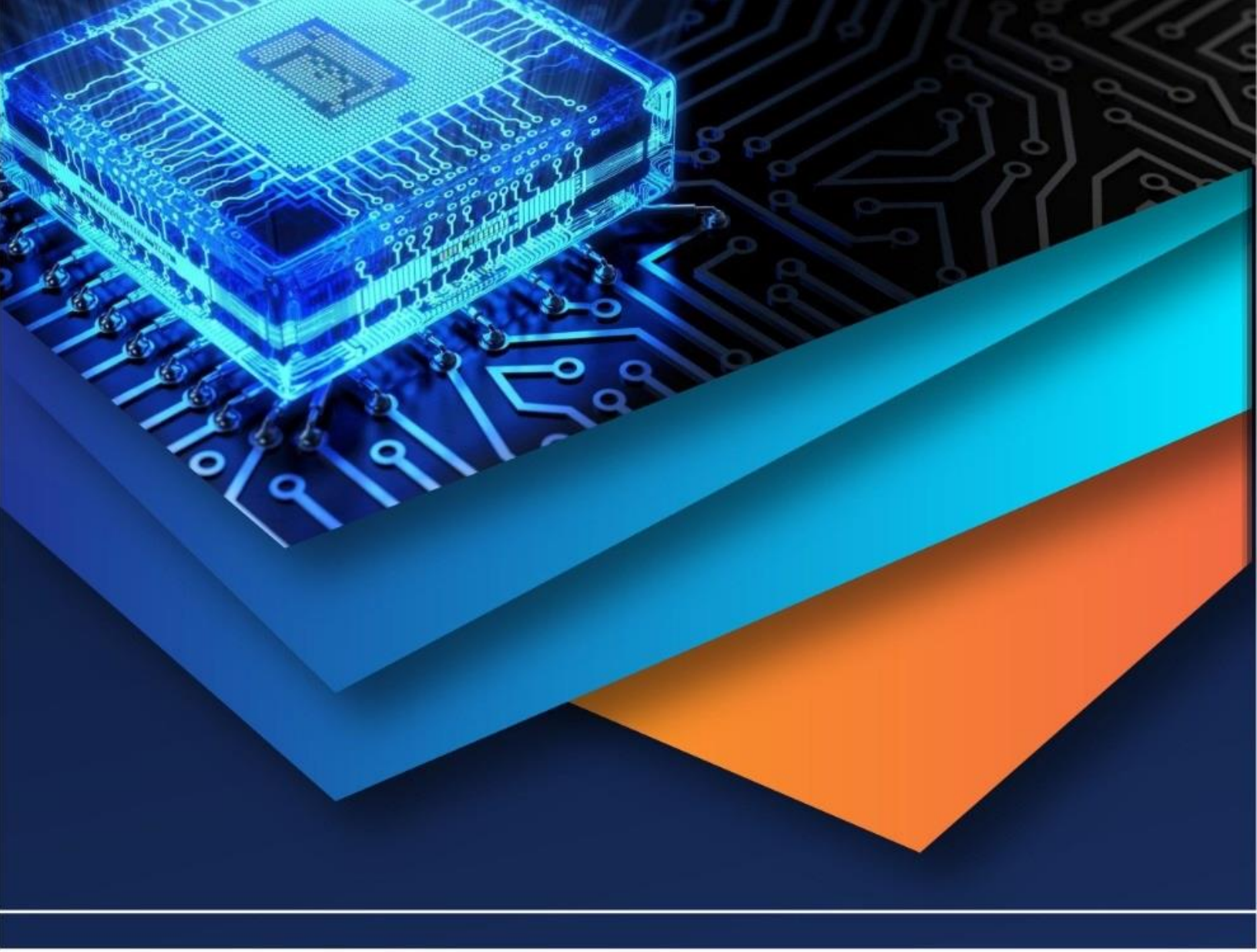
[16] Hetal P. Patel, Prof. Minubhai. B. Chaudhari, "Survey: Impact of Jellyfish On Wireless Ad-Hoc Network", in proceeding of INJCR’10, Volume.10, issue.5, no.2pp. 5-9, 2010

[17] Hepikumar R. Khirasariya, "Simulation Study of Jellyfish Attack in MANET (mobile ad hoc network) using AODV Routing Protocol", in proceeding of AISec’10, pp. 1-3, 2010

[18] BIJIT - BVICAM’s International Journal of Information Technology Bharati Vidyapeeth’s Institute of Computer Applications and Management, New Delhi, “A Novel Metric for Detection of Jellyfish Reorder Attack on Ad Hoc Network”.

[19] Proc. Int. Conf. on Computational Intelligence and Information Technology, CIIT, “Measuring the Impact of JellyFish Attack on the Performance of Mobile Ad Hoc Networks using AODV Protocol”.

[20] International Journal of Computer Trends and Technology (IJCTT) – volume 15 number 1 – Sep 2014, “Simulation of Jelly Fish Periodic Attack in Mobile Ad hoc Networks”.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY