iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** V **Month of publication:** May 2017

DOI:

www.ijraset.com

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

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Introduction to IEEE 802.11 Rogue Access Point Detection Mechanism Using Covert Channel

Prof. Kiran Somase[1], Akshay R. Shelke[2], Ankita S. Bhise[3], Rajat R. Balpande[4], Sagar D Bhusari[5]
[1,2,3,4] *Department of Computer Engineering, Dr. D. Y. Patil Institute and Technology, Pimpri, Pune, India*

Abstract - The problem of providing protection to the user from a rogue access point is a big problem today. To protect against the rogue access point through existing mechanism is by using IEEE 802.1x. However, it is difficult to use and impossible to quest. So, we are proposing a mechanism that will allow the users to protect their terminals before connecting to the rogue access points. This project presents the concept of access point authentication in terminals using covert channel over Transport Layer of TCP/IP reference model and it uses the timestamp field of beacon frame. So, in this project we are showing that without breaching the original standard of the frame, we can embed non-standard information on the timestamp field of 802.11 beacon frame.

Keywords: Rogue access point, Beacon frame, Permutation, Steganography, Covert channel.

I. INTRODUCTION

There are number of threats in networking that are damaging a secure network have been studied till now. Rogue Access Point is one of the most common and leading security threat in current network scenario. Many attacks such as DoS and data theft and other attacks can be implanted with the help of an RAP. If this issue is not properly handled at correct time then it could lead from minor network faults to serious network failure or a threat. Most of the current solutions that are used to detect RAPs are not automated and are dependent on specific wireless technologies. Varieties of solutions exist for detecting and eliminating RAP [5]. These solutions range from small, handheld devices to the large installations of network hardware and software, but all of them keep offering incomplete solutions. Hence, the problem of providing the protection to user from rogue access points has become a problem. This access point's presence is not broadcasted over the wire and can only be detected over-the-air. If the access point is declared as rogue it can be reported by MSS CLI, Network Director, MSS. To protect against these rogue access points using existing mechanism is IEEE 802.1x [1]. However, it is difficult to use. So, we are proposing a mechanism that will allow the users to protect the terminals before getting connected to rogue access points. This paper presents the concept of access point authentication in terminals using covert channel over transport Layer of TCP/IP reference model using timestamp field of beacon frame. This paper is showing a way by which without breaching the original standard, non-standard information can be embed on the timestamp field of 802.11 beacon frame [1]. An integrated solution for detection and elimination of RAP is created. This methodology [8] has the properties such as follows: (1) it does not require any specialized software as well as hardware; (2) the proposed system detects and completely eliminates the RAPs from network. This proposed solution is effective and low cost.

II. RELATED RESEARCH

The paper [1] presents the concept of using the covert channel which is used to authenticate access point. This covert channel is operated with the help of Beacon frames and timestamp field. It takes the advantage of the least significant bits of these fields. In this paper [2], the author has evaluated a new steganographic method called WiPad intended for IEEE 802.11 OFDM networks, whose functioning is based on insertion of bits into the padding of transmission symbols. It shows that the analysis for IEEE 802.11g 54 Mbps networks revealed that the capacity of WiPad equals 1.1 Mbit/s for data frames and 0.44 Mbit/s for ACK frames, which gives a total of almost 1.65 Mbit/s. It also reveals that this is the most capacious of all the known steganographic network channels. In this paper [3] it is shown that in a beacon frame there are few fields which can be utilized to carry additional non-standard information without breaching the original standard. Other than the fields proposed it is shown that the Length field of the IEs is also the potential candidate for the same. Using it, about 10 octets of additional non-standard information can be broadcasted without consuming any extra channel or network resources. Certainly, how to use these fields and what information is to be embedded depends upon the application requiring it. The purpose of this paper [4] is to detect and eliminate the rogue access points. Classification of rogue access point and analyse the related risk assessment. Also, rogue detection algorithm is proposed. The proposed solution is effective and low cost. It is designed to utilize the existing wireless LAN infrastructure. There is no need to

acquire the new RF devices or dedicated wireless detection sensors. They have demonstrated the experiments in the real system. The paper [5] shows the integrated solution for detection and counter attack of the rogue access points. Algorithm for rogue access point detection is designed. Risk assessment is analysed and rogue access points are classified. The solution is effective and low cost. It is designed to utilize the existing wireless LAN infrastructure. There is no need to acquire the new RF devices or dedicated wireless detection sensors. In this paper [6] it is shown that the fake access point detection system has been a major research area because of increased use of wireless network. In this paper [6] a fake AP detection method with its merits and demerits is presented. This method considers different but important parameters like SSID, MAC address and RSSI. The paper [6] also considers the parameters such as captures encrypted traffic data to analyse the network. This method overcomes the drawbacks of existing techniques. The experimental results show that the solution is cost effective, scalable, and easily deployable on any network. It is a lightweight solution without modifying network architecture. The study of this paper [7] shows that they are still away from a technique that will clearly identify the rogue access points. In real, such a technique that will collect constructive or precise information from network to determine whether a device is rogue or not is quite challenging as the network traffic is penetrate through multiple devices. So, there is need to discover technique that will be hybrid i.e. for wired and wireless. This will minimize the weaknesses of both wired and wireless techniques while maximizing their strengths. The paper [8] shows that the ease of setting up a successful rogue AP makes this form of wireless attack a particularly serious security problem in a network. While existing techniques that are present can alleviate this threat, they nonetheless require active participation on the part of the network administrator. In this paper [8], it presents a practical, timing based scheme for the end user to avoid connecting to rogue APs in a network. This is done without any assistance from the network administrator. The approach is implemented on commercially and is available for hardware evaluation. Various permutation algorithms have been studied in this paper [9] by Robert Sedgwick. Basic logic and working of the particular traditional algorithms have been explained with the examples. In this paper [10] the implementation of three most eminent permutation algorithms Bottom-Up, Lexicography, and Johnson-Trotter algorithms respectively. The implementation of each algorithm is carried out using two different approaches such as brute-force and divides and conquers. The paper [10] shows that algorithms codes are tested using a computer simulation tool which will measure and evaluate the execution time between the different implementations.

III. SYSTEM ARCHITECTURE

The presence of rogue access points is becoming a major concern for the organizations today. Administrators in organizations are worried because these rogue APs now introduce serious security threats. It is both simple and inexpensive to setup a rogue AP in a network from [4]. Without explicit authorization from a local network administrator, a rogue access point is installed on a secure network, whether added by a well-meaning employee or by a malicious attacker. If an attacker installs an access point they are able to run various types of vulnerability scanners, and the attacker remotely attacks from a reception area, adjacent to building or car park, rather than having to be physically inside the organization. From all this survey a better solution is designed for detecting rogue access point in a network. Beacon frame is continuously sent by AP to stations for every 100ms. In 64 bit timestamp field we can embed permutation key using 4 unused bits of timestamp field of 3 to 4 beacon frames. Changing this will not affect the network and it will be harden to be observed by malicious users. A permutation algorithm is used to generate random permutation numbers. These random generated numbers are used for connection purpose within a network which can be used as permutation keys at both access points and station's side. Before the connection, station will send a permutation key to the access point for verifying it as legitimate access point. The access point will receive this permutation key and decode it with the help of LSB technique of image steganography and the required key is sent back to the station. If these keys are matched at both the station and access point's side then the access point is declared as legitimate access point otherwise is declared a rogue access point. Once the AP is found as RAP all the requests by that RAP are ignored by the station. The image steganography is used to provide security for this mechanism. As decoding of image will take time by the RAP but even if that image is decoded the RAP will not able to provide the shared permutation key of the authorization connection. This makes the solution better to use as the free bits of timestamp field will be used for sending of these permutation key which will not affect the other working of the system. The memory will also not be wasted as these keys will be stored for only connection time period and will be discarded once the connection is established. So that the attacker will not be able to know which key was shared for the connection this makes the solution more secure.

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

IV. BEACON FRAME

To announce the availability of the network beacon frame in WLAN is used and it is also used for maintaining the tasks. At regular time intervals beacon frames are transmitted so that mobile stations can identify and find the network and it will lead to joining of that network.

Timestamp is a value which represents time on access point, which is in microseconds .When timestamp reaches to its maximum limit, it is then reset to 0.

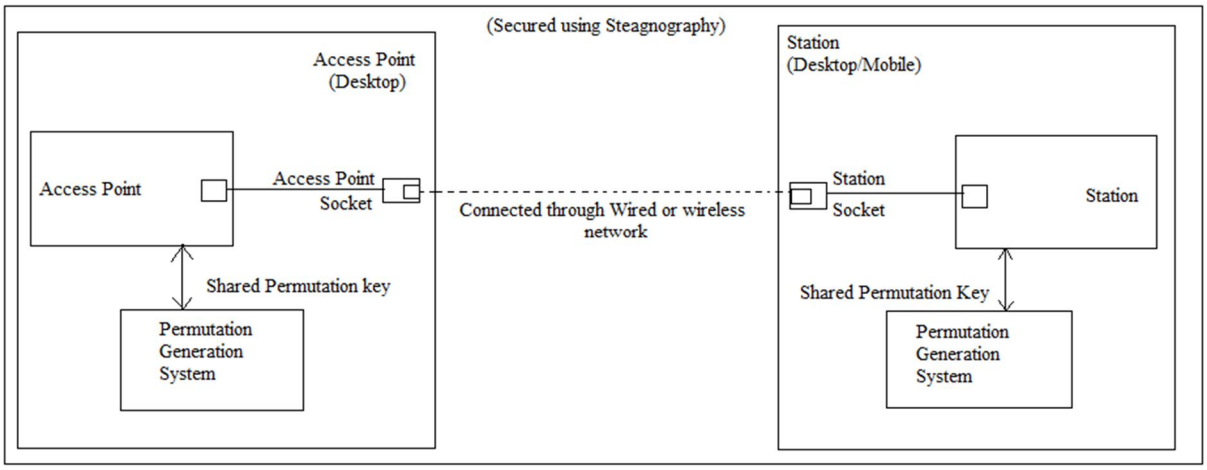


Figure 2. Beacon frame format

It is 8 Byte field of Beacon frame [3]. There are some free bits which can be used for computation. Our concept is to use those free bits of the Wi-Fi protocol stack without making any modification to the original Wi-Fi protocol stack. According to this concept in this timestamp field the code will be encrypted to generate the permutation key which will be protected using steganography mechanism. Such code will be generated on each device for authentication of access points. The image shows the modified beacon frame which includes the use of free bits of timestamp field for this approach to work.

V. CONCEPT OF MECHANISM

A. Beacon frame with permutation key

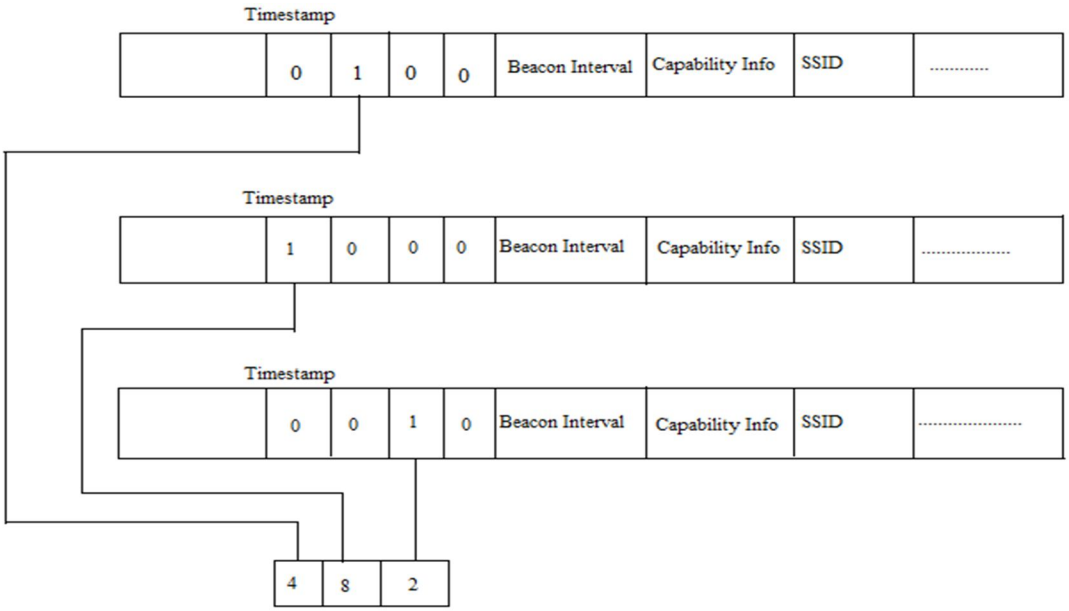


Fig: Data embedded in beacon frame

The above image is showing that permutation key is going to embed in most significant bit of the timestamp field bits. The twentieth bit those changes approximately every 10.48 seconds [1]. Thus the string length will be limited to approximately 400 bits (four bits per one frame, ten frames per second). In the above solution the station and access point must be synchronized and the station has to know the moment that when the permutation key transmission begins. In each beacon frame part of the key will be sent. If the attacker finds out that there is unusual activity is going on with the beacon frame and if these frames will be monitored only the part of frames will be attacked. Attacker will not be able to identify the whole key that is being sent to the access point.

B. Algorithm for generating permutations

1) *Johnson-Trotter algorithm*: The Johnson-Trotter algorithm [9] is a straight forward algorithm for generating permutations is a typical decrease by one algorithm:

find all permutations of size n1 of elements a1, a2, .., an-1
construct permutations of n elements as
append an to each permutation of size n-1
ii. for each permutation of size n-1
for k from 1 to n-1
insert an in front of ak

The straight forward implementation is very inefficient since it obtains all lower level permutations (permutations of size less than n). Instead of going through shorter permutations there is an algorithm which can be used to obtain all permutations of size n. This algorithm was designed independently by H. F. Trotter and S. M. Johnson. Mathematics of Computation and it is known as the Johnson Trotter algorithm from [9]. This algorithm works with directed integers. Each integer has directions from left or right. When an integer is greater than its immediate neighbour in the direction it is looking at then it is said to be mobile. Directed integers are represented by a structure that contains the integer and its orientation. The orientation can be represented as a binary value (Boolean value, 0/1 etc). The notation given represents the orientation by the symbols > and <.

C. The algorithm works as follows:

Initialize the first permutation with <1 <2 ... <n. While the last permutation has a mobile integer do find the largest mobile integer k swap k and the adjacent integer it is looking at reverse the direction of all integers larger than k
Example:
<1 <2 <3 <4 largest mobile element is 4
<1 <2 <4 <3 swap 3 and 4; largest mobile element is 4
<1 <4 <2 <3 swap 2 and 4; largest mobile element is 4
<4 <1 <2 <3 swap 1 and 4; largest mobile element is 3
after this step 4 has travelled all the way from right to left, being inserted in the shorter permutation n ‘123’. In the next step ‘123’ is processed to yield ‘132’

4> <1 <3 <2 swap 2 and 3; change direction of all greater than 3; largest mobile element is 4
<1 4> <3 <2 swap 1 and 4; largest mobile element is 4
<1 <3 4> <2 swap 3 and 4; largest mobile element is 4
<1 <3 <2 4> swap 2 and 4; largest mobile element is 3
after this step 4 has travelled all the way from left to right , being inserted in the shorter permutation ‘132’. In the next step „132‟ is processed to yield ‘312’.
<3 <1 <2 <4 swap 1 and 3; change direction of all greater than 3; largest mobile element is 4
<3 <1 <4 <2 swap 2 and 4; largest mobile element is 4
<3 <4 <1 <2 swap 1 and 4; largest mobile element is 4
<4 <3 <1 <2 swap 3 and 4; largest mobile element is 2
after this step 4 has travelled all the way from right to left, being inserted in the shorter permutation ‘312’. 3 also has travelled from left to right through ‘12’. In the next step ‘12’ is processed to yield ‘21’.

4> 3> <2 <1 swap 1 and 2; Change direction of all greater than 2; largest mobile element is 4

The algorithm will proceed transposing „4", and each time 4 reaches the opposite end „3" will be transposed. The last permutation obtained is <2 <1 3> 4>. It differs from the initial permutation just by one transposition (2 and 1). The algorithm has the following property i.e. any two successive permutations it generates are obtained from each other by a single transposition of adjacent elements. Algorithms with such property are called "minimal change" algorithms. The algorithm can be implemented to run in Θ(n!) time.

TABLE I

TIME COMPLEXITY (IN SECONDS) OF PERFORMANCE OF THIS ALGORITHM IN DIFFERENT LANGUAGES

Input Character	C	C++	Java	Android
3				0.001
4				0.002
5				0.014
6	0.0027	0.0043	0.127	0.035
7	0.0252	0.0248	0.529	0.39
8	0.1778	0.1233	2.12	3.21
9	1.4120	1.1514	20.41	31.12
10	14.069	12.155	209.85	

The table shows the analysis of time taken by different languages to perform the algorithm used for permutation generation for different combinations on Linux platform.

VI. FUTURE PERSPECTIVE

This solution can be implemented for real world use as the basic simulation of this approach gives positive output on Linux terminal. The solution will be implemented on Linux platform for creating actual access point and station on 802.11 protocol stack. We can also provide more permutation combinations for authentication and better security. Similarly, the mechanism can also be created to identify rogue stations.

VII. CONCLUSION

With the help of this technology a connection between the access point and station can be established with better security and more conveniently. Also, we can limit the number of users that can be connected. The covert channel is used to provide a secure path for transmission purpose. This mechanism will also detect the rouge AP so that station could only connect to the legal AP's. This also uses method of steganography for security purposes. This solution is cost effective, scalable and easily deployable on the network as no extra hardware is needed. It is a lightweight solution which is designed to use the existing WLAN infrastructure without modifying network architecture.

REFERENCES

[1] Krzysztof Sawicki, Zbigniew piotrowaski., The proposal of IEEE 802.11 network access point authentication mechanism using a covert channel, 2010-2012
[2] Szczypiorski K., Mazurczyk W., Hiding data in OFDM Symbols of 802.11 Networks , International Conferences on Multimedia Information Networking and Security(MINES), Nanjing, China, 2010.
[3] Information Embedding in IEEE 802.11 Beacon Frame Vishal Gupta, Mukesh Kumar Rohil from Birla Institute of Technology and Science Pilani, India, National Conference on Communication Technologies Computing CTNGC 2012
[4] Detecting Eliminating Rogue Access Point in IEEE 802.11 WLAN S.B.Vanjale, Amol K. Kadam, Pramod A. Jadhav Department of Computer Engg International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN) Volume-1, Issue-1, 2011
[5] Rogue Access Point Detection System in Wireless LAN, Ganesh B. Bandal, Vidya S. Dhamdhere, Siddharth A. Pardeshi, ISSN 2249-6343 , October 2012
[6] A novel approach for fake access point detection and prevention in wireless network SANDIP S. THITE1, SANDEEP VANJALE2 P. B. MANE3 1,2Department of Computer, BVDUCOE, ISSN(P): 2249-6831; ISSN(E): 2249-7943 Vol. 4, Issue 1, Feb 2014, 35-42
[7] Study of Different Rogue Access Point Detection and Prevention Techniques in WLAN Sachin R. Sonawane, Sandeep P. Chavan, Ajeet A. Ghodeswar,

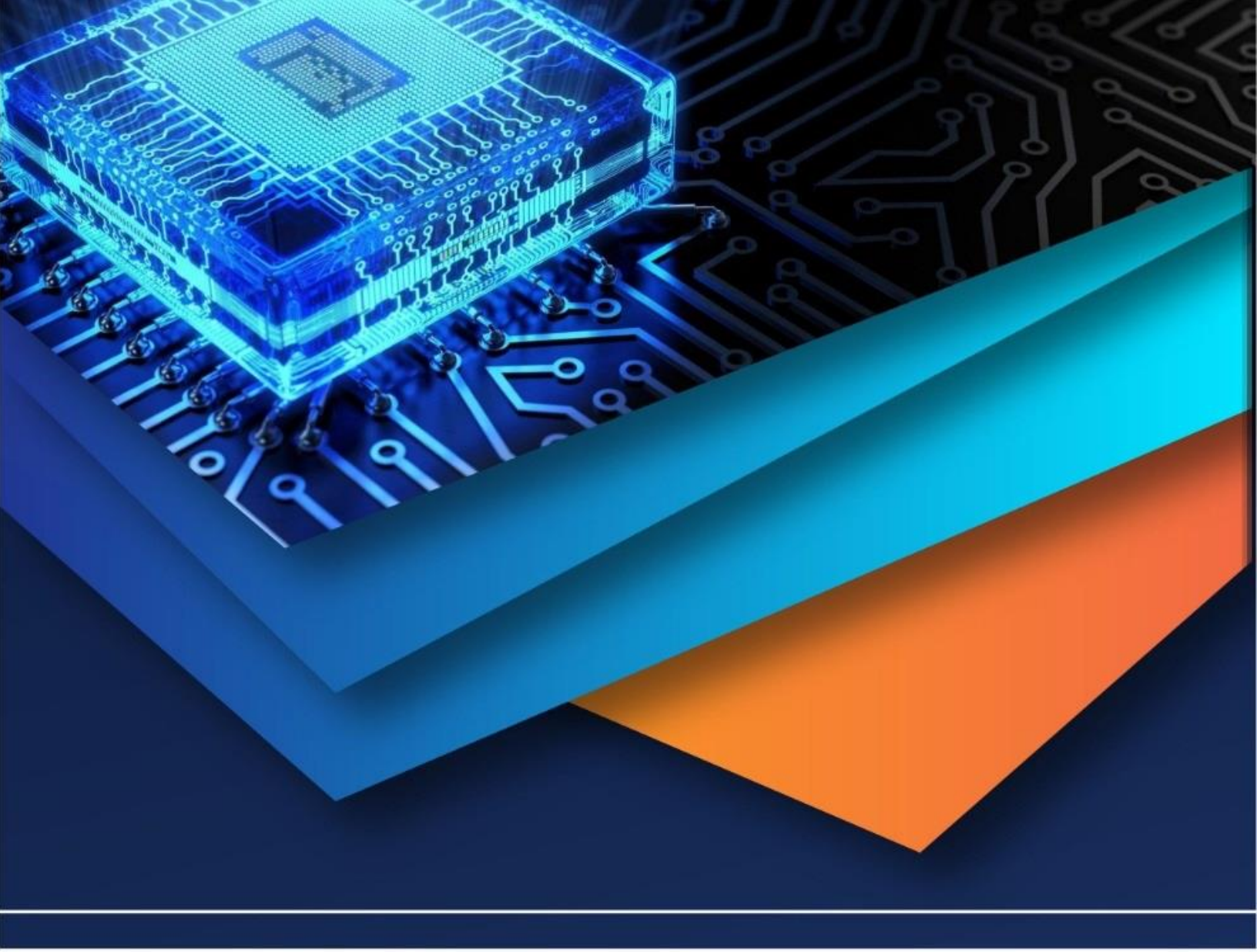
Volume 5 Issue V, May 2017
ISSN: 2321-9653

Sachin et al., International Journal of Advanced Research in Computer Science and Software Engineering 3(10), October -2013, pp. 1232-1237

[8] H. Han , B. Sheng, C. Tan Q. Li, and S. Lu, A measurement based rogue access point detection scheme, in the 28th IEEE International Conference on Computer Communications, Rio de Janeiro, Brazil 2009.

[9] Robert Sedgewick., Permutation Generation Methods*, June 1977

[10] Youssef Bassil., A Comparative Study on the Performance of permutation Algorithms, February 2012



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY