ISSN 2347 - 3983
Volume 7, No. 11 November 2019
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter137112019.pdf
https://doi.org/10.30534/ijeter/2019/137112019

Study and Analysis of Defense Techniques for Various Network Topologies

N V V N J Sri Lakshmi[1], P. Saleem Akram[2], V. Madhu Bhragavi[3], G. Harshika[4], A. Sravani[5]
Assistant Professor[1, 2], Graduate Student[3, 4, 5]
Department of ECE, Koneru Lakshmaiah Education Foundation, Guntur District, A.P, India
srilakshminandigattu64@gmail.com[1], saleemakramp@gmail.com[2],madhubhargavi98@gmail.com[3],
harshikagollavilli1998@gmail.com[4], sravaniaalapati10@gmail.com[5]

ABSTRACT

The era in which we live is the prime concern of security. The world has been computerized and protecting data from the attackers is really a crucial task. Several unauthorized network is entering into the authorized network. Designing a secured network is really a tough task. The layers which are affected due to hacking are data link layer and Network layer. This paper discuss 0about the type of attacks done by the attackers and counter measures for the attack. Cisco packet tracer is used to observe the path how data is sent and where data is moving.

Key words: Data Link Layer, Network Layer, Cisco Packet Tracer, Hacking.

1. INTRODUCTION

There is a tremendous increase in the computer security reported from statistics took place in 2018. Figure.1 represents the number of cyber-attacks [4] increased between 2006 and 2018.

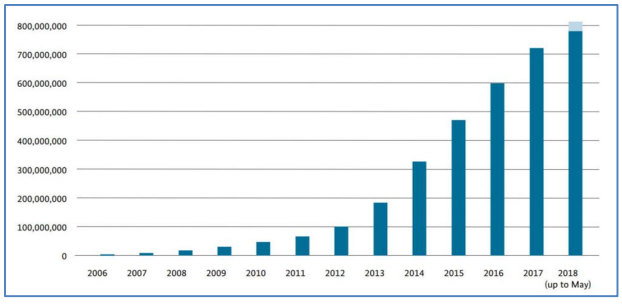

Figure 1: Attacks between 2006 and 2018

Along with the increase in attacks there is also increase in the sophistication. Many attacks seem to be user friendly and we don't bother about it and brief technical knowledge (figure 2) is enough to fight the attack. This carelessness leads the attackers to take advantage of various attacks.

Network attacks are an unwelcomed influence in present world and their count is increasing rapidly day by day. Figure 3 represents the change in attack on network traffic between the years 2015 to 2020.The dependence on information technology (IT) of human society has been increasing should make the people not to misuse it. Threats are the growing potentials which are making the network more vulnerable, they are caused by the increasing in technologies and by increase in the number of people who get advantage by abusing the system. Hackers, terrorists get more and more opportunities for attacks. This number is multiplied twice in industrial countries with critical infrastructure e.g. power supply, the health care center, trade (in particular e-commerce), the traffic system and the military protection.

The data packet transfer is initialized by application layer [25].These techniques can also be used in trending technologies like IOT [16-18].

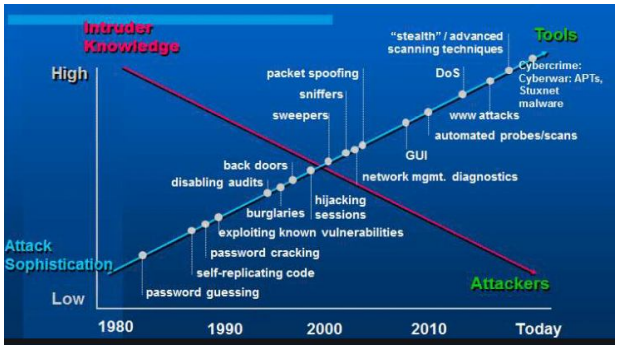

Figure 2: Graph on Attack sophistication and intruder technical knowledge

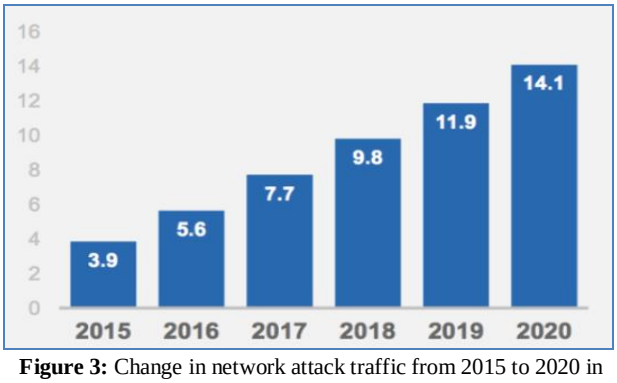

Figure 3: Change in network attack traffic from 2015 to 2020 in billions

2. NETWORK ATTACKS

2.1 Spanning Tree Protocol:

The Spanning tree protocol is a network protocol that builds the topology without looping for Ethernet networks. The work done by STP is to avoid bridge loops and produce results knows as broadcast radiation. Network design is allowed by spanning tree [5] to keep backup links for provision of fault tolerance if any active link fails.

Figure 4 Advantage of STP is if one path fails in the network it will not go back to the source node rather it checks the second best shortest path to reach the destination. This effect is caused due to hacking in data link layer [1] and network layer [2].This protocol [26, 27] is checked using cisco packet tracer [3].

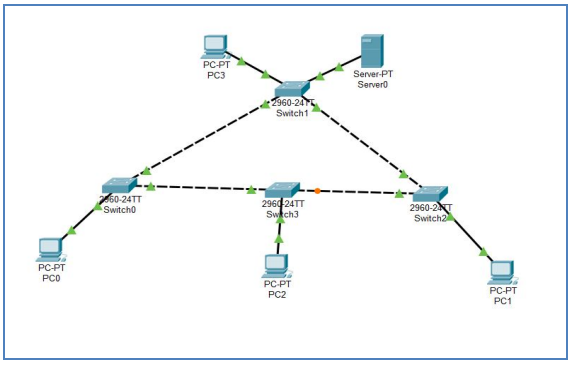

Figure 4: Network connection in Spanning tree protocol

The figure above represents the flow of packet from source to destination in the shortest path available. First it checks what the shortest path is available second it checks whether the path is set free to send packets or not if it is blocked it is sent by second shortest path which will in turn used for effective optimization of wireless sensor networks [14-15].

2.2 Dynamic trunking protocol:

DTP [6] represents Dynamic Trunking Convention. It is utilized to arrange a trunk interface and there are 4 sorts of DTP modes. They are getting to, trunk, dynamic auto, and dynamic attractive.

• Switch port mode get to: Puts the interface (get to port) into changeless non trunking mode and arranges the connection to change to a non-trunk interface. The interface turns into a non- trunk interface, paying little mind to check if the neighbor interface is a trunk interface or not.

• Switch port mode dynamic auto: This makes the interface can change over the connection into a trunk interface. The interface turns into a trunk interface only the neighbor interface is changed to trunk or alluring mode. The default switch port mode for fresher Cisco switch. Dynamic auto is the Ethernet interface. Note that a trunk will never shape if two Cisco switches are left to the regular default setting of auto.

	Access	Trunk	Auto	Dynamic Desirable
Access	Access	----------	Access	Access
Trunk	----------	Trunk	Trunk	Trunk
Auto	Access	Trunk	Access	Trunk
Dynamic Desirable	Access	Trunk	Trunk	Trunk

Figure 5: DTP Negotiated Interface Modes

• Switch port mode dynamic alluring: Makes the interface effectively endeavor to change over the connections to a trunk connect. The trunk channel is obtained from connection if the neighboring channel is set to trunk, alluring, or auto mode. This switch port mode on more seasoned switches are by default.

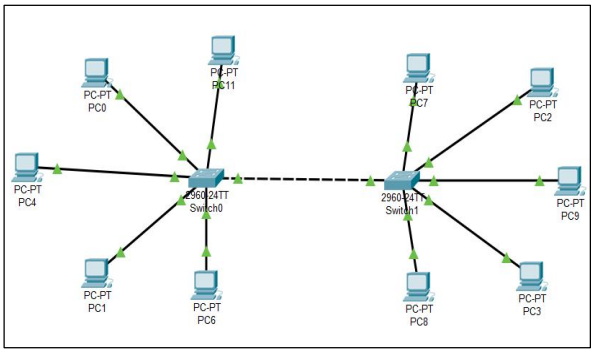

Figure 6: Network connection in Dynamic trunking protocol

Switch port trunk mode: Places the interface into perpetual trunking mode and consults to Change over the neighbor connection into a trunk interface. The interface turns into a trunk. Interface regardless of whether the neighbor interface is a trunk interface or not.

DTP is relied upon VTP [7] (Vlan Trunking Protocol).VTP conveys VLAN data to every one of the switches in a VTP space. In the event that VTP area is extraordinary, at that point it's impractical to have DTPs. Naturally all the cisco switch ports are in powerful alluring. To empower trunking from a Cisco change to a gadget that doesn't bolster dynamic trunking protocol, utilize the switch port mode trunk and switch port no negotiate interface setup mode directions. This makes the interface become a trunk yet not create DTP outlines. This is done using star topology this topology is mostly used in wireless sensor networks [11-13] and IOT [20, 22, 24].

2.3 Dynamic host configuration protocol:

A DHCP Server is a network server. This will automatically provide the IP address, default gateways etc. to the client.it will always depends on a protocol which is known as Dynamic Host configuration protocol i.e. DHCP[8]. A

DHCP server sends the parameters required for client. To communicate on the network without ,this the network administrators has to manually set up every client that joints the network, which can be very difficult to use ,mainly in the large networks server DHCP server always assign client with a unique IP address.

In Presence of DHCP, there is no need of manual assignment of IP addresses to new devices, due to its easy use and also the number of supporting people. DHCP is a default protocol and is used by the router and also the network equipment.

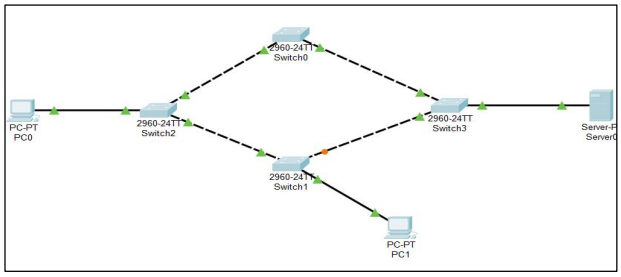

Figure 7: Network connection in Dynamic host configuration protocol

When we connected to a network, client is considered by the device and server is considered by the router. To connect it successfully to a network, the following steps should take place.

1. DHCP DISCOVER REQUEST
2. DHCP OFFER
3. DHCP REQUEST
4. DHCPPACK OR LEASE

1. If it is detected by client then it has connected to DHCP server, then it sends a DHCPDISCOVER request.
2. The request has been received by the router.
3. If the new device is accepted by the server, then it will automatically send the DHCPOFFER message to the client back again.
4. Then the client returns DHCPREQUEST message to the server, in the way of confirming manner that IP address will be used by it.
5. Acknowledgement message and confirmations are sent as a reply.

3. SWITCH CONFIGURATION

3.1 Switch configuration for spanning tree protocol:

Switch>en
Switch#show spanning-tree?
Switch#show spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 20481
Address 0004.9A29.ECA9
Cost 38
Port 1 (FastEthernet0/1)
Address 000A.F396.ED63
Hello Time 2 sec Max Age 20 sc Forward Delay 15 sec
Aging Time 20
Interface Role Sts Cost Prio.Nbr Type
---------- ----- ----- ---------- ---------- ----------
Fa0/3 Desg FWD 19 128.3 P2p
Fa0/1 Root FWD 19 128.1 P2p
Fa0/2 Altn BLK 19 128.2 P2p
fa0/4 Desg FWD 19 128.4 P2p
Switch#conf t
Switch (config)#spanning-tree vlan 1 root primary
Switch (config)#do show spanning-tree?
LINE
Switch (config)#do show spanning tree
VLAN0001
Root ID Priority 16385
Address 000A.F396.ED63
This bridge is the root
Address 000A.F396.ED63
Hello Time 2 sec Max Age 20 sc Forward Delay 15 sec
Aging Time 20
Interface Role Sts Cost Prio.Nbr Type
---------- ----- ----- ---------- ---------- ----------

Fa0/3 Desg FWD 19 128.3 P2p
Fa0/1 Desg FWD 19 128.1 P2p
Fa0/2 Desg BLK 19 128.2 P2p
fa0/4 Desg FWD 19 128.4 P2p
Switch(config)#

3.2 Switch configuration for dynamic trunking protocol:

Switch1#conf t

Switch1(config)#interface gigabitethernet fa0/3

switch1(config-if)#switchport mode dynamic desirable

switch1(config-if)#switchport mode trunk

switch1(config-if)#exit

3.3 Switch configuration for dynamic host control protocol:

interface fastEthernet0/3, changed state to up

Switch>;en

Switch#conf t

Enter configuration commands,per one line.

End with CNTL/Z.

Switch(config)#ip dhcp snooping

Switch(config)#ip dhcp snooping vlan 10 100

Switch(config)#int fa0/3

Switch(config-if)#ip dhcp snooping trust

Switch(config-if)#ip dhcp snooping trust Limit

rate 100

Switch(config-if)#end

Switch#show ip dhcp snooping

Switch DHCP snooping is enabled

DHCP snooping is configured on following

VLAN'S:

10,100

Insertion of option 82 is enabled

Verification of hwaddr field is enabled

Interface Trusted Rate limit

(pps)

…… …….. …….

FastEthernet0/3 yes 100

Switch#

4. SIMULATION RESULTS

4.1 Spanning tree protocol simulation:

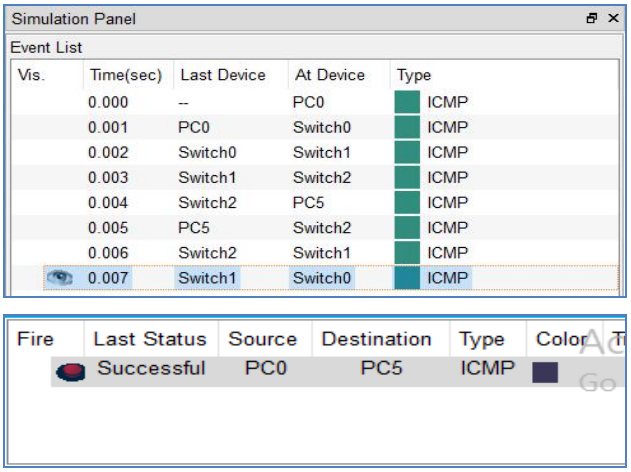

Figure 8: STP simulation

The above figure 8 represents the simulation of STP protocol(spanning tree protocol).In STP protocol there are source destination and type, i.e. ICMP[9] type. Here source is PC0 and destination is PC1, the packets which are transferred from source i.e., PC0 it should reach the destination i.e, PC1. Here attacks will block the route where the packets will go in order to hack the data. This algorithm is specially designed for avoiding bridge loops. If any shortest path fails this algorithm helps to find the next best path. In the 1st shortest path the packets can't reach their destination due to some attack. That attack is held between the switch and the network. The problem for this attack is there should be the configuration done between the switch and network then the packet can easily reach their destination without any attack or threats. In this STP protocol algorithm packets choose the next best path rather than first shortest path due to the no configuration done.

4.2 Dynamic trunking protocol simulation:

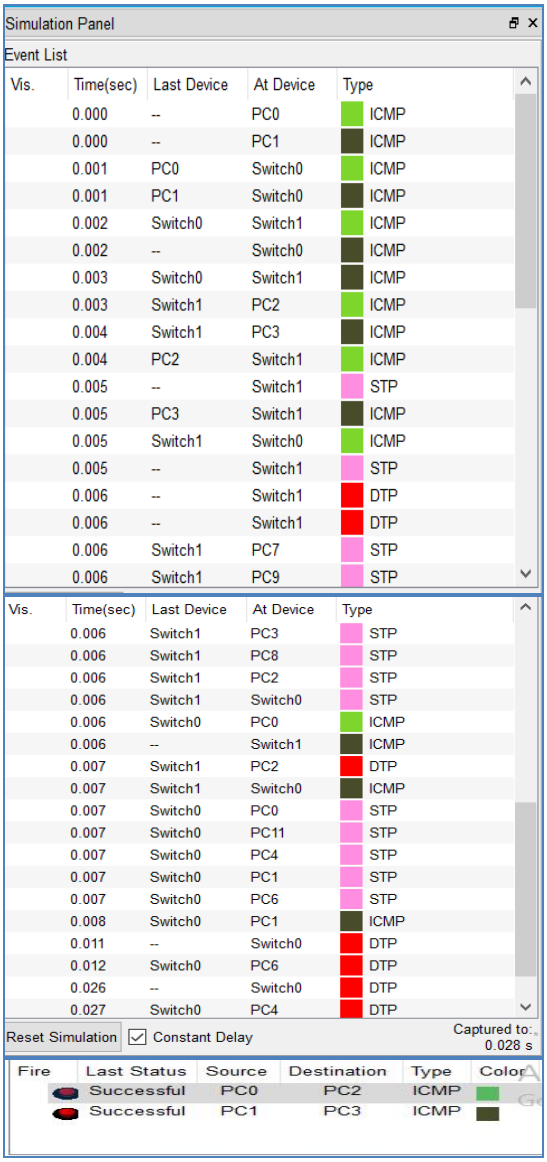

Figure 9: Simulation of dynamic trunking protocol

The above figure 9 represents the simulation of DTP (Dynamic Trunking Protocol).In DTP protocol there are source, destination and types (ICMP, STP, DTP) are present. Here in this protocol if we send any packets in pieces then the switch (i.e,switch0)collects all the packets and sends it in a multiple form to the other switch (i.e,switch1) and then transmits to the other users in multiple form. In this there is no attack as it is directly linked from switch0 to switch1.So there will not be a blocking of the route when the packets are sent. It sends the packets from PC0 to PC2, PC1 to PC3, and so on.

4.3 Dynamic host configuration protocol:

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC0	ICMP
	0.000	--	PC0	ARP
	0.001	PC0	Switch2	ARP
	0.002	Switch2	Switch0	ARP
	0.002	Switch2	Switch1	ARP
	0.003	Switch0	Switch3	ARP
	0.003	Switch1	PC1	ARP
	0.004	Switch3	Switch1	ARP
	0.004	Switch3	Server0	ARP
	0.004	PC1	Switch1	ARP
	0.005	Switch1	Switch2	ARP
	0.006	Switch2	PC0	ARP
	0.006	--	PC0	ICMP
	0.007	PC0	Switch2	ICMP
	0.008	Switch2	Switch1	ICMP
	0.009	Switch1	PC1	ICMP
	0.010	PC1	Switch1	ICMP
	0.011	Switch1	Switch2	ICMP

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.012	Switch2	PC0	ICMP
	0.715	--	Switch0	STP
	0.716	Switch0	Switch2	STP
	0.716	Switch0	Switch3	STP
	0.717	Switch2	Switch1	STP
	0.717	Switch2	PC0	STP
	0.717	Switch3	Switch1	STP
	0.717	Switch3	Server0	STP
	0.718	Switch1	PC1	STP
	2.717	--	Switch0	STP
	2.718	Switch0	Switch2	STP
	2.718	Switch0	Switch3	STP
	2.719	Switch2	Switch1	STP
	2.719	Switch2	PC0	STP
	2.719	Switch3	Switch1	STP
	2.719	Switch3	Server0	STP
	2.720	Switch1	PC1	STP
	4.310	--	PC0	DHCPv6

Fire	Last Status	Source	Destination	Type	Color
	Successful	PC0	PC1	ICMP	

Figure 10: Simulation of Dynamic host configuration protocol

By transferring the packet from source to destination figure 10 i.e. from pc 0 to pc 1, both MAC address and IP address of the destination should be known .if the destination is not Present then ARP will resolve the issue first and next the packet will be delivered to destination i.e. PC1.This technique can also be used in wireless antenna [6,10,23] applications.

ARP CACHE is a type of table it contains IP address and associated MAC address and ICMP type. Here packet is transferred from PC0 to switch 2 and from switch 2 it moves to switch 0 and from there it moves from switch 0 to switch 3.here it can't transfer to switch 1 from switch 3 and from switch 1 to destination because there is no configuration between the pc 1 and switch so it doesn't choose this path and it will choose the next best path.

5. CONCLUSION

From the above introduction, we have learnt and understood the network attack methods and their defense techniques. With this defense techniques performed above, we are able to construct more efficient attacker detection system and attacker protection system. When any unknown person enters our network attacker detection system gives us pre warning and attacker protection system will protect us from the unknown network.

REFERENCES

1. JAMES W. CONARD Services and Protocols of the Data link layer PROCEEDINGS OF THE IEEJ2, VOL. 71, NO. 12, DECEMBER 1983 https://doi.org/10.1109/PROC.1983.12781
2. A.K.Dwivedi,O.P.Vyas Network Layer Protocols for Wireless Sensor Networks:Existing Classifications and Design Challenges. International Journal of Computer Applications (0975 – 8887) Volume 8– No.12, October 2010 https://doi.org/10.5120/1255-1752
3. IMPLEMENTATION OF CISCO PACKET TRACER IN ADVANCE COMPUTER NETWORK, Sefer KURNAZ, Mohanad Mohammed ABDULKAREEM, Shadha Adnan YASEEN, Volume 2, No. 1 | Spring 2018, 33-47.
4. G.Balaji ,V.S.Hari Prassath , V.Sriram ISSUES BASED ON CYBER CRIME AND SECURITY. ISBN:978-93-87793-00-2
5. Dynamic Minimal Spanning Tree Routing Protocol for Large Wireless Sensor Networks Guangyan Huang1 , XiaoweiLi,andJingHe.DOI: 10.1109/ICIEA.2006.257220
6. Kusum Bhardwaj, Poonam Singh. Improving defence Mechanisms using packet tracer for switches and routers. ISSN No: 2456-6470.Volume-2,Issue-4. https://doi.org/10.31142/ijtsrd14246
7. Rajiv O.Verma, S.S. Shriramwar 2013 International Conference on Communication Systems and Network Technologies Effective VTP Model for Enterprise VLAN Security, April 06 - 08, 2013 , ISBN: 978-0-7695-4958-3 https://doi.org/10.1109/CSNT.2013.95
8. Rich Woundy, Kim Kinnear, Dynamic Host Configuration Protocol (DHCP) Leasequery.Published in RFC 2006 DOI:10.17487/rfc4388
9. Md. Ataullah, Naveen Chauhan. An efficient and secure Address Resolution Protocol, DOI: 10.1109/SCEECS.2012.6184794
10. Saleem Akram P., Ramana T.V., "Stacked electromagnetic band gap ground optimization for low profile patch antenna design",International Journal of Engineering and Advanced Technology, ISSN:22498958, Vol No: 8, Issue No:3, 2019, pp:146 – 154.
11. Rao, K. R., Kumar, T. R., ; Venkatnaryana, C. (2016). Selection of anchor nodes in time of arrival for localization in wireless sensor networks doi:10.1007/978-81-322-2671-0_5

12. Sahiti, V., Raghava Rao, K., ; Mohan Rao, K. R. R. (2016). Hashing technique data optimization for low power consumption in wireless sensor network. Indian Journal of Science and Technology, 9(17) doi:10.17485/ijst/2016/v9i17/93101
13. Saleem Akram, P., ; Ramana, T. V. (2019). Two dimensional beam steering using active progressive stacked electromagnetic band gap ground for wireless sensor network applications. Journal of Computational and Theoretical Nanoscience, 16(5-6), 2468-2478. doi:10.1166/jctn.2019.7918
14. Bhatt, P., Akram, P. S., ; Ramana, T. V. (2015). A novel on smart antennas to improve performance in wireless communications. Paper presented at the International Conference on Signal Processing and Communication Engineering Systems - Proceedings of SPACES 2015, in Association with IEEE, 187-190. doi:10.1109/SPACES.2015.7058245
15. Saleem Akram, P., ; Venkata Ramana, T. (2019). A novel approach of microstrip fed planar monopole antenna for wsn applications at 2.4ghz ism band. International Journal of Scientific and Technology Research, 8(8), 665-669.
16. Abdul A.M., Krishna B.M., Murthy K.S.N., Khan H., Yaswanth M., Meghana G.,Madhumati G.L., IOT based home automation using FPGA ,2016, Journal of Engineering and Applied Sciences, Vol: 11, Issue: 9, pp: 1931 - 1937, ISSN 1816949X
17. Narayana M.V., Dusarlapudi K., Uday Kiran K., Sakthi Kumar B.,IoT based real time neonate monitoring system using arduino,2017 Journal of Advanced Research in Dynamical and Control Systems,Vol:9, issue:Special issue 14,pp: 1764-1772,DOI: ,ISSN: 1943023X
18. Gadde S.S., Ganta R.K.S., Gopala Gupta A.S.A.L.G., Raghava Rao K., Mohan Rao K.R.R. .,; Securing Internet of Things(IoT) using honeypots “, 2018, Microsystem Technologies ,Vol: 24 ,Issue: 3 ,pp: 1609 to:: 1614 ,DOI: 10.1007/s00542-017-3563-x ISSN: 9467076
19. Ravikanth, B., Akram, P. S., Ashlesha, V., ; Ramana, T. V. (2017). Tuning operating frequency of antenna by using metasurfaces. Paper presented at the International Conference on Signal Processing, Communication, Power and Embedded System, SCOPES 2016 - Proceedings, 2064-2068. doi:10.1109/SCOPES.2016.7955811
20. Gopi Krishna P., Srinivasa Ravi K., Hareesh P., Ajay Kumar D., Sudhakar H. .,; Implementation of bi-directional blue-fi gateway in IoT environment “, 2018 International Journal of Engineering and Technology(UAE) ,Vol: 7 ,Issue: ,pp: 733 to:: 738 ,DOI: ,ISSN: 2227524X
21. Muzammil Parvez M., Shanmugam J., Mohan Rao K.R.R., Lakshmana C., Shameem S..,; Alive node and network lifetime analysis of DEEC protocol and EDDEEC protocol “,2018, International Journal of Engineering and Technology(UAE) ,Vol: 7 ,Issue: ,pp: 661 to:: 664 ,DOI: ,ISSN: 2227524X
22. Pavithra T., Sastry J.K.R. .,; Strategies to handle heterogeneity prevalent within an IOT based network “, 2018, International Journal of Engineering and Technology(UAE) ,Vol: 7 ,Issue: 2 ,pp: 203 to:: 208 ,DOI: 10.14419/ijet.v7i2.7.10293 ,ISSN: 2227524X
23. Devi Susmitha, N., Sowmya, S., Akram, P. S., ; Ramana, T. V. (2017). Tuning of L-C meta-material structure for antenna applications. Paper presented at the International Conference on Signal Processing, Communication, Power and Embedded System, SCOPES2016-Proceedings,1845-1850. doi:10.1109/SCOPES.2016.7955764
24. Poonam Jain S., Pooja S., Sripath Roy K., Abhilash K., Arvind B.V. .,; Implementation of asymmetric processing on multi core processors to implement IOT applications on GNU/Linux framework “, 2018, International Journal of Engineering and Technology(UAE) ,Vol: 7 ,Issue: 1.1 ,pp: 494 to:: 499 , ,ISSN: 2227524X
25. Rambabu K., Venkatram N. .,; Traffic flow features as metrics (TFFM): Detection of application layer level DDOS attack scope of IOT traffic flows “, 2018, International Journal of Engineering and Technology(UAE) ,Vol: 7 ,Issue: 1.1 ,pp: 554 to:: 559, ISSN: 2227524X
26. Anuka Pradhan, Biswaraj Sen "A brief study on Contention Based Multi-Channel MAC Protocol for MANETs", International Journal of Emerging Trends in Engineering Research (IJETER), Vol 6, No 12, pp 74-78, Dec 2018. https://doi.org/10.30534/ijeter/2018/016122018
27. Kyeongjoo Kim, Jihyun Song, Minsoo Lee " Real-time Streaming Data Analysis using Spark", International Journal of Emerging Trends in Engineering Research (IJETER), Vol 6, No 1, pp 1-5, Jan 2018. https://doi.org/10.30534/ijeter/2018/01612018