IJNRD.ORG ISSN : 2456-4184

INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG

An International Open Access, Peer-reviewed, Refereed Journal

International Research Journal IJNRD Research Through Innovation

Future obligations In relation to incorporating IPv6 into the Internet of Things (IoT).

[1] **Dr. Rajeev Kaushik,** Professor, CSE Department, RD Engineering College, Duhai, Ghaziabad, UP, India.

Abstracts: The rapid advancements in computer networking technology and related developments have transformed our world to the point where an internet connection is deemed essential for functionality and relevance. With the emergence of IPv6 alongside the enhanced capabilities of 4G and 5G networks, there is a notable shift away from legacy network protocols. IPv6 is progressively supplanting existing protocols, paving the way for a future where all devices are interconnected through multiple pathways, free from the constraints of ISP sub-netting. However, this ubiquity of connectivity presents significant challenges for maintaining stable communication. In such a scenario, where constant connection to the global network is imperative, the need for seamless, uninterrupted interaction without human intervention arises—a requirement often fulfilled by the advent of advanced Artificial Intelligence systems.

Keywords: *IPv6,(AI)Artificial Intelligence, Mobile computing, IoT, AS(autonomous system).*

I. Introduction

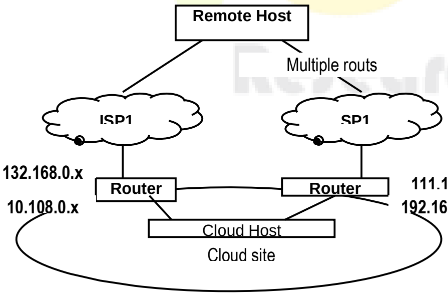
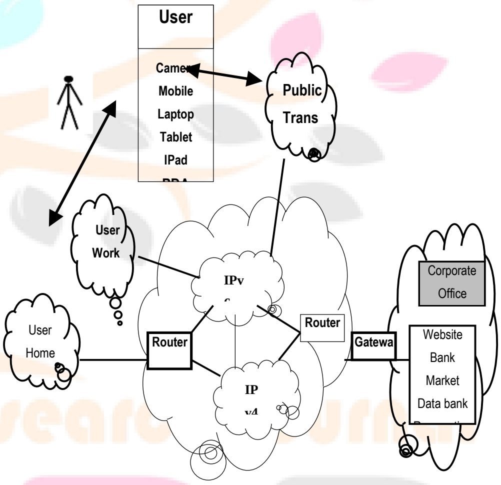


Fig.1 Multihoming

Multihoming is the method to connect the remote computing device with the help of multiple inter undependable paths. This is helpful to create fault tolerant and load balanced network.

IPv6 is changing the world very rapidly; it will overcome the problem of IPv4 for exhausted of IPv4 address problem. Today world is dual IPv4/IPv6 **cloud** world and it is dependent on ISP based structure since the shortage of IPv4.



2. IPv6 Support Cloud

Combination of Public Cloud as well of private cloud, but soon this will not be remains same there will be total cloud based as compare to individual infra structure. India is 46% ready for IPv6. The devices will get its unique IP address and that may be the ISP independent as shown in Fig.2.

1.1 Moving computing enabled devices

Moving networked computing devices such as mobile, laptops, tables, GPS enabled devices on IPv6 [6] protocol, are increasing dramatically. Mobile computing devices has three parts: Mobile hardware, Mobile communication, and Mobile software. The first part includes communication related matters in ad-hoc and infrastructure networks in term of wireless communication, Mobile phone network communication, and as well as communication properties, protocols, data formats and concrete technologies. The second part is on the hardware, like mobile devices or device components. The third is about the those s/w which are design in such way that they keep on work flawlessly while the device is keep on changing it location from one network to another network.

2. Problem & Discussion

There are various concerns which are very important to be discussed and to work on for future issues avoidance. As IPv6 enabled Multihoming based cloud computing is going essential. When such node become on which is using Multihoming, Multihoming will creates more than 1 rout may be 4 to 5 links routs depending on the how much ISP and direct links, he has connected and how much those ISP in multiple ways, are connected to the rest of world.

When the sensors are in numbers with huge information has to be transmit every moment. Combined power of IPv6 and IoT increases the routing table entry and creates an additional routing load on routing devices such as routers and Gateways. Multihoming is also used to increase severity of various attacks like DOS denial of services, spamming and such others [8][9]. These loads can be understood easily, but also be reasons for slow internet performance and often congestion. Mobile/Sensors devices had enhances the effect of Multihoming by two reasons.

1. In IoT based cloud world Mobile computing provides more time to user/devices/sensors to be remaining connected, user can be connected to the network all the time while user is not on the sitting place.
2. IPv6 enabled IoT based Multihoming creates multi paths for a multiple locations.

Device/Sensors create multi paths using Multihoming. Since it is authorized separately for both networks, a malicious program resides in the device which is infected at the previous location. This program will easily scan the new network available. Since such malicious program is sitting in devices/ sensors which is authorized in current network, it can create problem in authorized network.

Since this malicious program has two networks accessibilities, it can easily sideline the securities of both network by combine two networks, behaving as router of two networks. Using multi path mechanism it can makes fool remote machine easily and easily put treble in the security of remote host.

User has mobile data card which provide him a 10 mbps 4G connection 5G (more than 1Gbps). Some application like torrent and other downloader are creating multi routs. The IPv4 model is facing serious challenges, some of them are following are other concern:-

a). Route Congestion & network overloading **b).** Virus Attack **c).** Broadcast.

Ad-hoc network faces several types of attack such as Location Disclosure, black hole, replay, wormhole, denial of services, routing table poising, rushing attack, masquerading, virus and passive listening with traffic analysis. These are direct challenges to IPv6 enabled Multihomed IoT with extended severity may bring down the network to standstill.

To mobile machines/sensors, it is very difficult to judge an unknown network. Whether stay on IPv4 network or shift to IPv6 in new network. These will creates a situation in which, many packets be routed from the both network because both network will be there.

On checking connectivity at various places and monitored response times. A lot of disconnection were noticed and observed slow response times while moving during the transmissions using remote desktop logins, a lot of disconnection faced while entering in new network. Some location showed, connected system behaved abnormally. For example sometime packets forwarded to unknown gateways and then lost without reply or sometime the response time reaches in thousands milliseconds. Sometime browser stuck-up and it needed to reboot the system to established fresh connection. Sometime server refused to get fresh connection since the early remote login was active which we connected from early location. It has been seen that some unattended connections were still open when we returned to same locations. At overlapping zone device start change IP addresses for both overlapping networks so frequently to work properly, due auto connection condition started to connect one network than other network as the strength increases and decrease.

IoT with IPv6 will be more effective in Mobile computing since IPv6 will provide individual unique IP address to AS device. It will force to use the IPSec, which will reduce the risk of the packet to interrupted and interpreted in the channel.

DHCP configuration of IPv6 greatly helps to produce network easily. These will more easily implementation of Mobility without changing IP in different Networks. Due this device may able to work with it unique IP address rather than network dependent IP. But there should require more effort to implement such thing, need more open network that allow any type of IP to get connected with WAN. Proxy and NAT requirement will not be there, due to this, hopes will be reduced in each packet transmission.

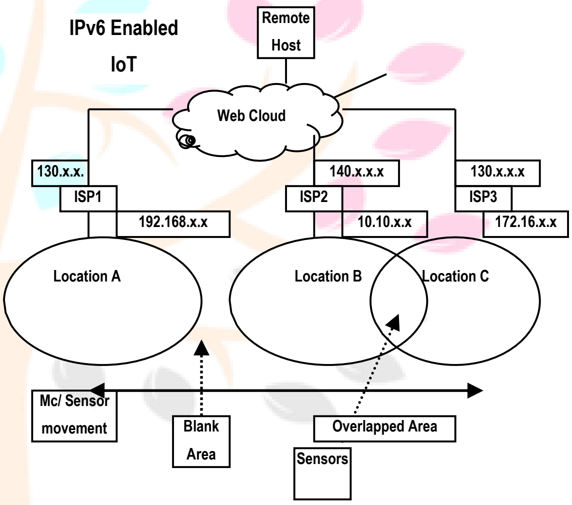


Fig. 3 User / Device Movement

User who is mobile and keeps on changing locations is major concerns in future since technology is going to provide a implementable solution to all moving sensors in bulk ways. There are two locations A and B, which is far away, and there in between is middle location C where none of the two network reach well in good strength. A and B overlapped at C place, the network strengths of both continuously varies in area of C, which is good enough in size.

A moving AS start works at location-A user get connected to remote host (RH) via network. The IPv4 IP are used, due shortage of IP, everywhere the NAT is used and user works with address LAN address at different places. As fig.3 depict user get a IP of 192.168.x.x series at location A, while user moved to location B user get the IP address 10.10.x.x and in location C user gets IP series 172.16.x.x, this way, user gets a different IP at all different locations. This creates problem at remote host where user after authentication from location A and remote host authorizes the user on the basis of IP address. Since user does not have real IP, user's router or gateway IP will be authorized at remote host. When user reaches in the no signal area user's all connection remains open for location A. The multi paths are established and it will remain open. When user reaches location B user get new IP and user's router/gateways will used as authorized computer but the remote host will treat it as unauthorized connection and abruptly force to close connection.

While user reach at overlapping area the situation can further worsen since as the laptop keep on changing position, signals strength start changing of both network, as the strength increase

IJNRD Research Through Innovation

of the B location, the DHCP of B location gives it LAN IP of series 10.10.x.x and user get connected that LAN. But soon C strength increase and laptop get IP of series The speed of a rout is effected by the speed of slowest routing point.

Many websites are not yet IPv6 enabled. Windows like OS are using IP **Teredo Tunneling** Pseudo-Interface as conversion method. This tunnel creates a packet of IPv4 from IPv6 and then again IPv4 to IPv6. This conversion consumed a heavy computing resource. IPv4 router has to route those packets which have less data payload and great addition packet related information.

They will contain IPv6 header inside IPv4 data packet payload. So in actual they are doing data communication in very less efficient way. Lot of time will be consumed in IP conversion at source and destination node. Due to Multihoming huge computing resources like CPU cycle and RAM memory will be consumed. Multihoming brings packets from various streams, a complex and time consuming process creates additional overhead compare to a single stream, this will be problematic in cloud computing where the simultaneous the multiple connection has been running to satisfy the multiple users all around the world specially in world of AI supported AS . But the

Now going on move from one network to another network. While moving to new network the LAN ip is also new, in such condition the Public network real IP is also new and the new LAN address is also new. It become difficult to block new real IP since there may lot of other user is doing the work with that real IP. When IPv6 will be in full swim the difficulty will multiply in many folds. Social software such as Facebook, twitter, , WeChat, Whatapps, TV online, News with online videos GPS systems, Security cameras, live video conferencing. The sensors used in IoT to control devices such as fan, lighting, AC, Cooler, TV, house / Organization will make everything automatic and remote control/managed but also produce a unsubstantial congestion.

3. Conclusion

It is assumed that cloud based IoT has to take care of critical and difficult issues in coming time. The users will be connected all the time with help of social cloud chat software, such as Skype, Whatapps and other GPS based software. User will use online TV on.

Multiple users will place website in own laptops/mobile phones and there website will move with them and they will avoid cloud computing and use of cloud based web space, due to money reason and security reasons. Implementation of IPv6 will easily available the freedom to make user's device visible to everybody on the internet at any point of time. This will make a shift in the current protected world of firewalls and security system due to isolation mechanisms.

3.1 Future scope of the IPv6 and IoT with multi path system is going to be massively scalable. The working of all routers is still working on best path basis. They all exchange information keep in mind, the best in term any cost like time/ hops the one best path only, not IPv6 enabled IoT. The routers in internet simply start data sending on best and do not select multiple paths and other hand, major OS do not implement the Multihoming facilities yet. We have seen or noticed that as soon one network come in effective the OS simple turned out weak signal network without bothering, even though that network might had maintaining many connection. This can be seen in mobile phone / move devices such as apple pad, tablets, as WiFi get connected, it switch off mobile data, network of carrier. So even to network are available it complete switch over to strong network as instant as possible, it do not try to use both network. Still a big change is required in all available hardware/ mainly in software. The major work will come when the IPv6 will be implemented fully. There will be numerous and complex There will be a situation when a moving device contain virus and start virus Attack, is creating lot of traffic. Mobile Multihoming increases effects of attacks. There will be a great concern how the firewall and other control will be implemented on such open network in future when device will be available without LAN and Firewall. While using Mobile computing the firewall implemented on premises LAN will not allow user to access organization resource when he goes on WAN, by real IP in mobile Computing. Still in IPv4 all real IP are controlled by the ISP, the same may be applied in the IPv6device with multi homing will face problem when some of the packet is routed through IPv4 network and some packet will routed on IPv6. There may be situation even better rout available on either IPv4 or IPv6 network but the system will not able to use it while entering in to new unknown network. This will create under utilization condition.

Software will produce heaviest load on the networks. Some of them are Skype, Youtube, especially with high definitions videos, Chatting and Messaging when attack is start on a cloud providing the cloud will block the Pulblic IP via which the attack is going on, but it is difficult to block a mobile device.

issues, when two heterogeneous IPv4 and IPv6 worlds will be there with mobile sensors/devices such as IP enabled camera, GPS, PDA, iPad, transport system and such others devices. The new simple, more effective and secure protocols will require. The increase dependency on computer and Internet with required availability to access information 24x7 all around the year time span, at all location of the earth, had created a lot of pressure on the computing infrastructure especially on computer inter connected networks. So we see, **future Responsibility of IoT is important and lot work had to be done for handling huge future requirement.**

4. REFERENCES

[1] Batiha K. Improving IPv6 Addressing Type and Size. International Journal of Computer Networks & Communications (IJCNC). 2013; 5(4): 41–51p

[2] Khan, M.A. Saeed, Y. Asif, N. Abdullah, T. Nazeer, S. Hussain, A.[2012] "Network Migration And Performance Analysis Of Ipv4 And Ipv6", M GC. University Faisalabad, Pakistan, European Scientific Journal March edition vol. 8, No.5 ISSN: 1857 – 7881 (Print) e - ISSN 1857- 7431.

[3] N. Jagan Mohan Reddy, G.Venkareshwarlu, et al. "Wireless Electronic Display Board Using GSM Technology", International Journal of Electrical, Electronics and Data Communication, ISSN: 2320-2084 Volume-1, Issue-10, Dec-2013

[4] G. Huston, "An Update on Multihoming in IPv6 – Report on IETF Activity", Proceedings of RIPE49

[5] J. Abley., "IPv4 Multihoming Practices and Limitations" (work in progress), IETF Internet-Draft, January 2005

[6] G. Huston, "Commentary on Inter-Domain Routing in the Internet", IETF RFC 3221, December 2001

[7] G. Huston, "Analyzing the Internet's BGP Routing Table", The Internet Protocol Journal, vol. 4 no. 1, T. Bu, L. Gao and D. Towsley, "On Routing Table Growth", Proceedings of Global Internet Symposium, 2002

[8] K. K. Sharma and Dr. Rakesh Dube, Multihoming architecture used in attacking mail and web servers, Journal of Global Research in Computer Science (JGRCS), Volume 2, No. 5, May 2011, page 116-119, ISSN: 2229-371X

[9] K. K. Sharma and Dr. Rakesh Dube, Loading on routers due to multihoming architecture, Journal of Mathematics & Computing System, July-December 2011, pp 63-66, ISSN: 0976-9048

[10] Karpilovsky, E., Gerber, A., Pei, D., Rexford, J., Shaikh, A.: Quantifying the Extent of IPv6 Deployment. In: PAM.