ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2014

IPv6 Based Mobile Cloud Computing to Compact with Key Dilemma

Jessie Pauline Jeyapriya

Principal, CSI College for Womens, Madurai, Tamilnadu, India

ABSTRACT: Mobile cloud computing is the combination of cloud computing and mobile networks to bring benefits for mobile users, network operators, as well as cloud computing providers. A mobile cloud approach enables developers to build applications designed specifically for mobile users without being bound by the mobile operating system and the computing or memory capacity of the Smartphone and PDA Devices. Mobile cloud computing center are usually accessed via a mobile browser from a remote web server, typically without the need for installing a client application on the recipient phone. In there was some problems occurs due to its mobility and dynamic environment. The major concern deals with these perceptions are security, link failure, mobile traffic, routing, power consumption, etc. In this presented scheme, issues arise with this mobile cloud computing can be prevail over by IPv6 (Internet Protocol Version 6). IPv6 is the newest version of the Internet Protocol (IP), the communications protocol that affords an identification and location system for computers on networks and routes traffic across the Internet. In this paper, the IPv6 based Mobile Cloud Computing will be built up to defeat the major issues of security, dynamic routing concept and link failure during the mobility of the nodes within the networks. By using IPv6 it offers diverse security services at the IP layer and therefore, offers protection at this (i.e. IP) and higher layers. The key dilemma such as link-failure and dynamic routing in the mobile computing will be defeat over by the dynamic routing protocol and cross over approach for link-failure detection in this paper.

KEYWORDS: Mobile Cloud Computing, IPv6, key dilemma, Security, Link-Failure, dynamic routing

I. INTRODUCTION

Cloud computing refers to the delivery of computing resources over the Internet. Instead of keeping data on your own hard drive or updating applications for your needs, you use a service over the Internet, at another location, to store your information or use its applications. Doing so may give rise to certain privacy implications. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications.

Mobile cloud computing (MCC) at its simplest, refers to an infrastructure where both the data storage and data processing happen outside of the mobile device. As referred in [1] Mobile cloud applications move the computing power and data storage away from the mobile devices and into powerful and centralized computing platforms located in clouds, which are then accessed over the wireless connection based on a thin native client. Mobile devices face many resource challenges (battery life, storage, bandwidth etc.). Figure 1 shows the architecture of mobile cloud computing. Mobile cloud computing provides mobile users with data storage and processing services in clouds, obviating the need to have a powerful device configuration [3] (e.g. CPU speed, memory capacity etc), as all resource-intensive computing can be performed in the cloud.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2014

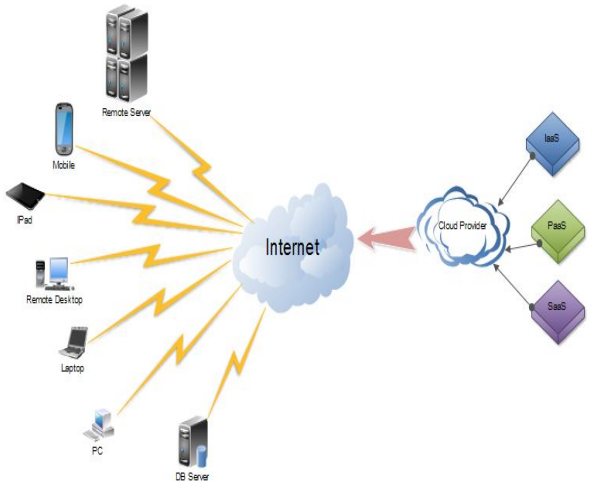


Figure 1: Architecture of Mobile Cloud Computing

MCC is still in its upbringing and it is a promising technology [2]. It provides many benefits, but its openness lead to more expansion. A novel proposal and protocols can be tied to this virtual environment to afford superior benefits or to solve the existing problems. To make these superior benefits one protocol can be use is IPV6.

The Internet Protocol (IP) is the most widely used communications protocol. Because it is the most pervasive communication technology, it is the focus of hundreds of thousands of IT professionals like you. Because so many people rely on the protocol, the safety of communications is top of mind. The security research that is performed on IP is conducted by both benevolent and malevolent people [5]. All the security research has caused many patches and adjustments to IP, as it has been deployed internationally. In hindsight, it would have been better if deeper consideration were given to the security of the protocol before it was extensively deployed.

IPv6 or IP version 6 is the next generation Internet protocol which will eventually replace the current protocol IPv4. IPv6 has a number of improvements and simplifications when compared to IPv4. The primary difference is that IPv6 uses 128 bit addresses as compared to the 32 bit addresses used with IPv4. This means that there are more available IP addresses using IPv6 than are available with IPv4 alone. For a very clear comparison, in IPv4 there is a total of 4,294,967,296 IP addresses. With IPv6, there are a total of 18,446,744,073,709,551,616 IP addresses in a single /64 allocation.

IPv6 is the second network layer standard protocol that follows IPv4 for computer communications across the Internet and other computer networks. IPv6 offers several compelling functions and is really the next step in the evolution of the Internet Protocol [7]. These improvements came in the form of increased address size, a streamlined header format, extensible headers, and the ability to preserve the confidentiality and integrity of communications. The IPv6 protocol was then fully standardized at the end of 1998 in RFC 2460, which defines the header structure. IPv6 is now ready to overcome many of the deficiencies in the current IPv4 protocol and to create new ways of communicating that IPv4 cannot support.

IPv6 will eventually be just as popular as IPv4, if not more so. Over the next decade as IPv6 is deployed, the number of systems it is deployed on will surpass those on IPv4. While early adopters can help flesh out the bugs, there are still many issues to resolve. IPv6 implementations are relatively new to the market, and the software that has created these systems has not been field tested as thoroughly as their IPv4 counterparts. There is likely to be a period of time where defects will be found, and vendors will need to respond quickly to patching their bugs. Many groups are performing extensive testing of IPv6, so they hopefully can find many of the issues before it is time to deploy IPv6.
IPv6 solves a set of problems that are related to the interaction between nodes that are attached to the same link. IPv6 defines mechanisms for solving each of the problems such as security, link-failure and dynamicity. Due to the mobility

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2014

and dynamic environment leads the mobile cloud service to deal with this key dilemma. To compact with these key dilemma the remuneration of the IPV6 will be implemented with this mobile cloud computing.

II. RELATED WORK

The conception of Mobile Cloud Computing (MCC) emerging from the technology cloud computing with the mobile applications as declared in [1]. The mobile devices integrate with the cloud computing to structure an environment and defeat over the hindrance to upgrade the performance of the cloud service. In these context [1] [2], the major leads and the main shortcoming occurs in the mobile cloud computing would be clearly declared. This paper concluded the architecture of the MCC and the main issues that arises in that environment.
In this research, the mobile applications which are integrates within the cloud service and their work survey where defined [3] [7]. By using these mobile applications, there would be some issues occurs due to the openness and also this paper examined the unique approaches to get rid of these issues. The challenges over the mobile cloud service which integrates with mobile applications.
IPv6 is the novel version of Internet Protocol next to the IPv4. The features and benefits of the IPv6 are referred in [3]. The next generation of the Internet Protocol (IPv6) is developed to implement and improve the communication between the different networks. This context involved in the research of the IP to move on to the next version named IPv6. The key issues occurred in earlier version IPv4 and the refinement of the issues by the novel version of IPv6 is defined in this paper.

The IPv6 have many of the features which acclimatize to the different networks [5] such as wireless, sensor networks, and rooftop networks. The key dilemma of the wireless networks occurs due to its mobility and dynamicity, the mobile cloud service hindrance with the many challenges and issues [8]. To defeat over these challenges the mobile cloud needs a narrative version of Internet Protocol known to be IPv6. IPv6 builds an overlay architecture for a wireless networks [4] to deals with major issues and challenges over the MCC with the assist of IPv6. The major security issues and the security refinement can be clearly defined in the context [10].

The security challenges of various network environments have been overcome by one of the features of IPv6 named IP Sec (IP Security). In the context of [9] [11], the features of IP sec and its application leading have been declared and concluded the IP sec in mobile applications would provide good performance. This paper [9] makes strategy design for IPSec in IPv6 protocol, and established by the network security of IPSec afforded. The performance analysis and the application revelation were examined. In this paper [11] depicts an investigation of the recital overheads caused by the dispensation and hole necessities of IPSec when defending mobile IPv6 (MIPv6) signalling. Signalling between the mobile nodes and the home agent (HA) in a large-scale reference scenario is considered.

The other issues of MCC will be discussed [13] [15], the link detection within the wireless networks would be clearly defined. The major involvement of the offered work in the paper [13] was introduced a new approach for a route link detection in wireless networks. The successful hardware implementations using cross-layer approach will extends the battery life of the mobile nodes in the networks. The context of [17] [18] make a survey and provide a conclusion regarding the routing protocols in wireless networks. In the context of [18] the preferred protocols are evaluated on the source of multiple parameters, which include packet delivery ratio, packet loss, network lifetime, and control overhead using variable number of nodes and speeds. The intention of this paper [17] is to generate classification of the ad hoc routing protocols, and to review and compare delegate examples for each class of protocols. We attempt to expose the requirements considered by the different protocols, the resource limitations under which they operate, and the design decisions made by the authors.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2014

III. DILEMMA CLASSIFICATION

Security

In the present cloud issues that create interesting security problems. Identify a few security issues within this framework. Propose some approaches to addressing these issues. Cloud computing definitely makes sense if your own security is weak, missing features, or below average. Ultimately, if the cloud provider's security people are "better" than yours (and leveraged at least as efficiently), the web-services interfaces don't introduce too many new vulnerabilities, and the cloud provider aims at least as high as you do, at security goals, [8] then cloud computing has better security. The most security problems stem from loss of control, lack of trust and multi-tenancy with the cloud computing. These problems exist mainly in third party management and self-managed clouds still have security issues. User access control rules, security policies and enforcement are managed by the cloud provider. Consumer relies on provider to ensure Data security and privacy, Resource availability, Monitoring and repairing of services/resources.

Link-Failure Detection

Mobile cloud services operating in wireless environments require fast detection of link failures in order to enable fast repair. In preceding cloud service, the cross-layer failure detection can reduce failure detection latency significantly. In the scrutiny of Mobile cloud network, the rapidity of nodes is a key property of mobility. The network is unstable when the nodes move faster. In the analysis, [8] link failure rate is widely used to modelling the stability of a wireless network. An analysis of a basic mobility model and shows that the link failure rate is positively correlated with the average speed of nodes in this model is presented. Though this result is based on a mobility model with many restrictions, a simulation evaluation suggests that the result still holds in the popular random waypoint model and random direction model.

Dynamic Routing

Dynamic routing is a networking technique that provides optimal data routing. Unlike static routing, dynamic routing enables routers to select paths according to real-time logical network layout changes. In dynamic routing, [8] the routing protocol operating on the router is responsible for the creation, maintenance and updating of the dynamic routing table. In static routing, all these jobs are manually done by the system administrator.

In this paper, the IPv6 protocol is implemented with the mobile cloud computing to defeat over these dilemma. IPv6 have further reimbursement when compared to the IPv4, by using these benefits in mobile cloud service the key dilemma will be trounce in this paper.

IV. PROPOSED TECHNIQUE

Mobile devices are connected to the mobile networks via base stations that establish and control the connections and functional interfaces between the networks and mobile devices. Mobile users' requests and information are transmitted to the central processors that are connected to servers providing mobile network services. The subscribers' requests are delivered to a cloud through the Internet. In the cloud, cloud controllers process the requests to provide mobile users with the corresponding cloud services.

Computation offloading migrate large computations and complex processing from resource-limited devices [6] (i.e., mobile devices) to resourceful machines (i.e., servers in clouds). Remote application execution can save energy significantly. Many mobile applications take advantages from task migration and remote processing. Improving data storage capacity and processing power: Mobile Cloud Computing (MCC) enables mobile users to store/access large data on the cloud. MCC helps reduce the running cost for computation intensive applications [9]. Mobile applications are not constrained by storage capacity on the devices because their data now is stored on the cloud. Keeping data and application in the clouds reduces the chance of lost on the mobile devices. MCC can be designed as a comprehensive data security model for both service providers and users: Provide security services such as virus scanning, malicious code detection, authentication for mobile users. With data and services in the clouds, then are always available even when the users are moving.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2014

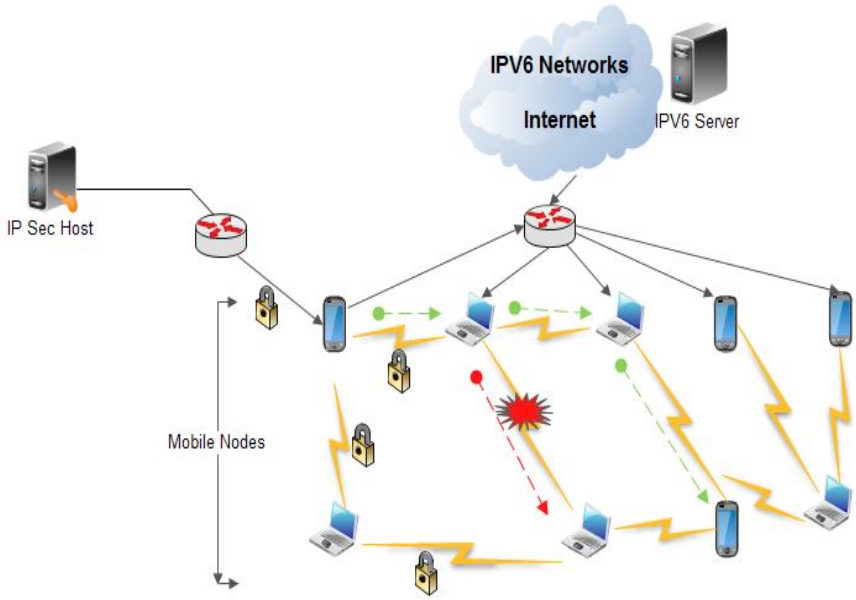


Figure 2: Proposed Architecture

In this presented technique, the major dilemma designations that are occurred due to the openness of this Mobile cloud computing can be detected and resolved with the aid of IPv6. IPv6 have many features when compared to the older version IPv4. In this paper, the features of IPv6 will be used to repair the key dilemma occurred in the Mobile cloud computing. The proposed technique elucidates the refinement of the dilemma classification.

Dilemma Refinement

IP Security (IP sec)

The security issues in the existing mobile cloud service will be defeat over by the key feature of the IPv6 known to be IP sec (IP Security). Internet Protocol security (IPSec), which provides protection of IPv6 data as it is sent over the mobile cloud network. As shown in [10] IPSec is situating of Internet standards that uses cryptographic security services to afford confidentiality, authentication and data integrity. IPSec traffic is encrypted and confined IPSec traffic cannot be deciphered without the encryption key. IPSec traffic is digitally signed with the shared encryption key so that the receiver can verify that it was sent by the IPSec nodes over the cloud network. IPSec traffic contains a cryptographic checksum that incorporates the encryption key. The receiver can verify that the packet was not modified in transit.

Using IPSec, participating mobile devices can achieve data confidentiality, data integrity, and data authentication at the network layer [11]. It offers various security services at the IP layer and therefore, offers protection at IP and higher layers. These security services are, for example, access control, connectionless integrity, data origin authentication, protection against replays, confidentiality (encryption), and limited traffic flow confidentiality. IPSec allows the encryption of only particular application protocols while others are simply authenticated. In addition, one can also specify that communication toward specific IP addresses will be protected, whereas unprotected communication can be used for other destination IP addresses. The flexibility and transparency of this protocol makes it possible to mold a security configuration for every need. IPSec uses the features, such as using an Authentication Header and the Internet Key Exchange (IKE), are incompatible with NAT—another reason to move toward IPv6 and reduce the use of NAT gateways.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2014

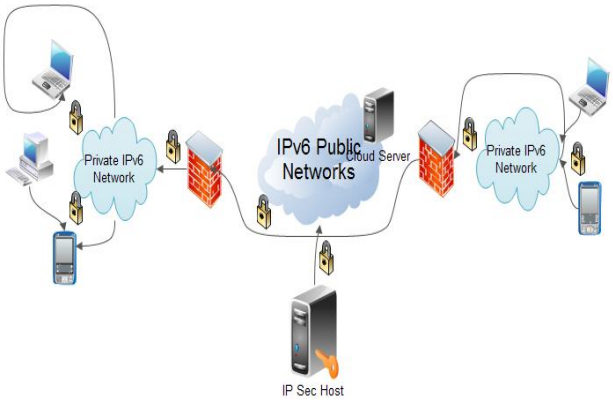


Figure 3: IP Security in Mobile Cloud using IPv6

The IPSec virtual tunnel interface (VTI) provides site-to-site IPv6 crypto protection of IPv6 traffic. Native IPv6 IPSec encapsulation is used to protect all types of IPv6 unicast and multicast traffic. The IPSec VTI allows IPv6 routers to work as security gateways, establish IPSec tunnels between other security gateway routers, and provide crypto IPSec protection for traffic from internal networks when it is sent across the public IPv6 Internet [12]. IPSec has two different modes: Transport mode (host-to-host) and Tunnel Mode (Gateway-to-Gateway or Gateway-to-host). In transport mode, the payload is encapsulated (header is left intact) and the end-host (to which, the IP packet is addressed) unwrap the packet. In the tunnel mode, the IP packet is entirely encapsulated (with a new header). The host (or gateway), specified in the new IP header, unwrap the packet. Note that, in tunnel mode, there is no need for client software to run on the gateway and the communication between client systems and gateways are not protected.

Cross Layer Approach for Link-Failure Detection

One of the immense disputes of mobile cloud computing is require to sustain services such as real-time applications that are rather perceptive to packet loss, transmission errors and delay using an expertise IPv6. The networks should design with backup links, derelict nodes and alternate routes to insure that can quickly recover from detected link failure. Detection of link failure in cloud service is an important dilemma. Previously routing protocol's *neighbor discovery mechanisms* is used for detection of link failure in IPv6 [13]. In this proposed technique, the *cross layer approach* is used to detect the link-failure in mobile cloud environment to carry out well-timed detection of failed link.
In the existing technique, the neighbor discovery mechanism, the HELLO message is used. All the nodes of the networks send HELLO messages to its neighbored nodes within its communication assortment. A Link is implicit in superior condition when after receiving number of HELLO messages on that link and that link can be used for packet forwarding. In other words, the link-failure is detected, when the deficiency of HELLO messages on that link for explicit time period. Real-time use cannot use this approach for detection of link-failure because huge amount of delay occurs.
In the cross layer approach, when a MAC frame is received then the acknowledgement is sent for that frame. The frame is retransmitted when the acknowledgement is not received [15]. The link is assumed to be failed when the number of retransmission is performed and the frame is lost. Detection of link failure is performed by taking into account the number of failed delivery occurred in MAC layer along with the information about transmission errors. The advantage of cross layer approach over simple approach of neighbor discovery is the fast finding of link failure.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2014

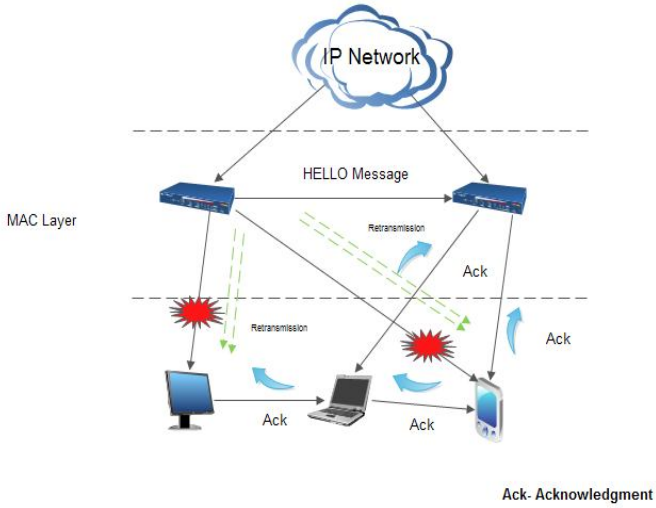


Figure 4: Cross layer approach to detect Link-failure

Location-based Routing Protocol

Routing in Mobile cloud using IPv6 is demanding due to differentiate from other wireless networks like MANET or WSN. It is not feasible to construct a dynamic addressing format for a huge number of mobile nodes. Thus, [16] [18] traditional IP-based protocols may not be applied to this mobile cloud computing like IPv6. In this network, sometimes receiving the information is more important than perceptive the IDs of which nodes sent the information. In distinction to distinctive communication networks, almost all applications of cloud networks need the flow of mobile device data from multiple sources to a particular node. The task of finding and maintaining routes in mobile cloud is nontrivial since energy restrictions and sudden changes in node status (e.g., failure) cause numerous and volatile topological changes.

In this proposed technique, *the location-based routing* will be implemented to make the dynamic routing in mobile cloud using IPv6. In location based routing, mobile nodes locations are demoralized to route data in the network. In this routing concept, the mobile nodes are addressed by means of their locations [17]. The distance between the neighboring nodes can be anticipated on the basis of incoming packet potency. To save energy, some location based schemes demand that nodes should go to sleep if there is no activity. More energy savings can be obtained by having as many sleeping nodes in the network as possible. In this paper, the important location based routing protocol is used named as *GPSR (Greedy Perimeter Stateless Routing).*

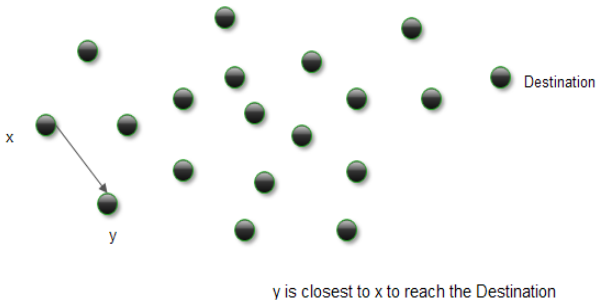


Figure 5: Greedy Forwarding

GPSR allows nodes to figure out who its closest neighbors are that are also close to the final destination the information is supposed to travel. To calculate a path, [19] GPSR uses a greedy forwarding algorithm that will send the information to the final destination using the most efficient path possible. If the greedy forwarding fails, perimeter forwarding will

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2014

be used which routes around the perimeter of the region. A node just has to remember the location of neighbors within one-hop. Routing decisions can be dynamically made. Assuming the mobile nodes know their own locations the Greedy forwarding algorithm will try to find the closest router which is also the closest to the final destination.

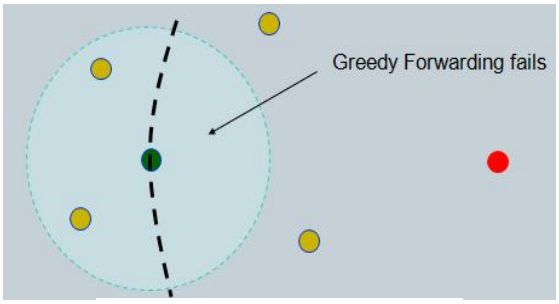


Figure 6: Greedy Forwarding fails

If the network is dense enough that each interior node has a neighbor in every 2π/3 angular sector, Greedy Forwarding will always succeed. However, the greedy forwarding algorithm can fail.

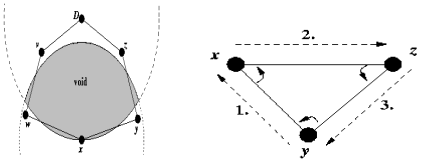


Figure 7: Perimeter routing

When the Greedy Forwarding algorithm fails, the Perimeter Forwarding algorithm will be used. Apply the right-hand rule to traverse the edges of the void and find a path using the topology's perimeter. [20] The Perimeter Forwarding Algorithm uses a longer path to the destination so the perimeter forwarding algorithm less efficient and cannot be used alone. Putting Greedy Forwarding and Perimeter Forwarding together makes the final GPSR which will use the necessary algorithm(s) to find the best path in a given topology.

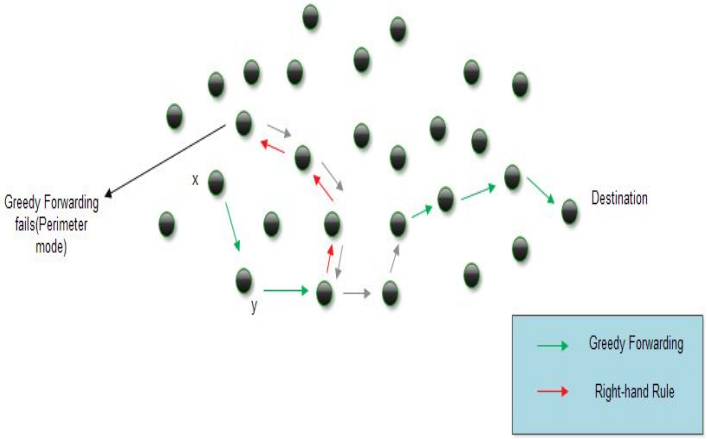


Figure 9: GPSR Routing

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2014

V. SIMULATION AND RESULTS

As discussed in this paper, the IPv6 engaged a major responsibility to defeat over the challenges and dilemma of the MCC. Regarding to the discussion the simulation results provide good performance of MCC with IPv6 when compared to the existing scheme (IPv4, NDM).

Performance of MCC	IPv4	IPv6
Bandwidth measured	35.7 Gb/s	31.2 Gb/s
Throughput	38.06 Gb/s	34.09 Gb/s
Send Energy Utilization	35%	30%
Receive Energy Utilization	40%	34%
Bits Transfer	125 Kbps	125 Kbps
Failure link detection	20 /s	35 /s
Packet Delivery Ratio	120 /s	150 /s

Figure 8: IPv6 Performance over IPv4 in MCC

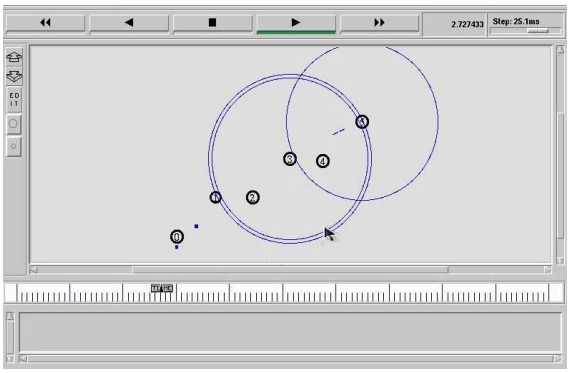


Figure 9: Routing in MCC

The above figure (8) & (9) shows the performance results of the IPv6 features in MCC. The features include IP sec, cross layer approach in link detection and finally the packet delivery ratio during the routing in MCC. The simulation of GPSR in MCC is illustrates in figure (9). In the routing of MCC, the network size will increase synchronously where ever and when ever. In that situation the GPSR routes all the nodes according to the location of the nodes is simulated in this figure.

VI. PERFORMANCE ANALYSIS

This paper entirely focuses on key dilemma of the mobile cloud networks. Thus, the key dilemmas are refined using novel version of Internet Protocol known as IPv6. This proposed architecture of this networks resulting in good security constraints, link-failure detection and better dynamic routing by using the features of IPv6. The performance of the security constraints using *IPSec* (IP Security) is measured in the means of Time Interval and the Bits Per sec to refine the network traffic of the mobile cloud service is shown in the Figure 9(a).

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2014

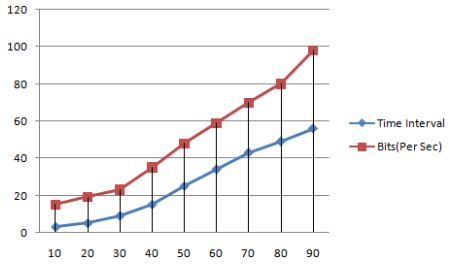
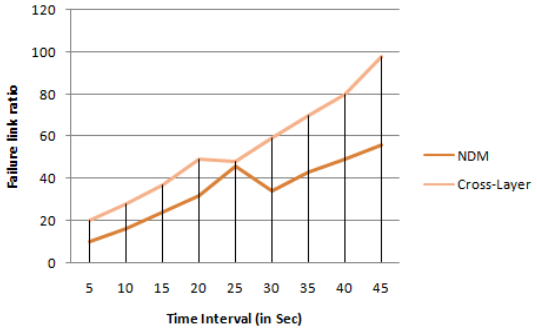


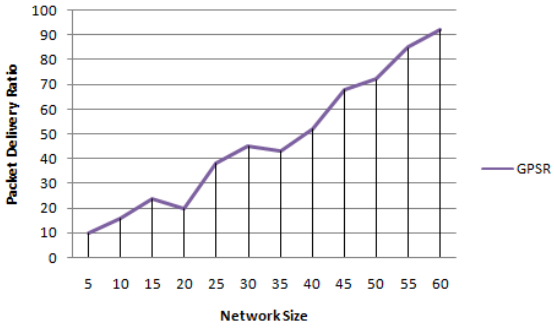
Figure 9: (a) Network Traffic

Detection of link-failure during the packet forwarding or transmitting messages is detected using the approach- *Cross Layer*. The performance analysis for the link-detection in the cloud environment using IPv6 is shown in the Figure 9 (b). This figure shows that the failure link detected within the particular time interval using cross layer approach. The cross layer gives better performance than the existing approach of Neighbor Discovery Mechanism (NDM).



(b) Failure Link Ratio

The figure 9 (c) shows the packet delivery ratio of the mobile cloud using IPv6 and the GPSR routing protocol to forward packets through the neighbor nodes when the network size increases and the mobility rate will be increased in level. Thus this routing protocol gives good performance in packet forwarding during routing whenever the network size is increased.



(c) Packet Delivery Ratio

VII. CONCLUSION

Finally, this paper concluded that the major issues occurred in the mobile cloud computing due to its mobility and dynamicity will be refined using the novel version of IP known to be IPv6. This paper examined the features of the IPv6 in the mobile cloud services and implement the techniques in this network to overcome the key dilemma occurred such as security, link-failure and dynamic routing which are discussed in this paper. The IP sec in IPv6 is worn to avoid the security dilemma of the mobile cloud. The detection of link-failure and the dynamic routing can be implemented

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2014

using the cross layer approach and the GPSR routing protocol. This routing protocol makes the mobility rate good in the mobile cloud services.

In future work, the other major issues of the mobile cloud computing will be refined using IPv6 and various routing protocol and approaches can be used in dynamic routing to avoid malicious behaviours. Also can implement this features of IPv6 in various types of networks named sensor networks, rooftop networks.

REFERENCES

[1] Hoang T. Dinh, Chonho Lee, Dusit Niyato and Ping Wang, " A survey of mobile cloud computing: architecture, applications, and approaches ", Wireless Communications and Mobile Computing - Wiley, vol.13, Issue 18, pp. 1587–1611, 2013.

[2] Jibitesh Mishra, Sanjit Kumar Dash, Sweta Dash, "Mobile-cloud: A framework of cloud computing for mobile application", Lecture Notes of the Institute for Computer Sciences, Social- Informatics and Telecommunications Engineering, vol. 86, pp. 347-356, 2012.

[3] Pragya Gupta, Sudha Gupta, "Mobile Cloud Computing: The Future of Cloud", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 1, Issue 3, 2012.

[4] Dijiang Huang ; Arizona State Univ., Tempe, AZ, USA ; Zhibin Zhou ; Le Xu ; Tianyi Xing, "Secure data processing framework for mobile cloud computing", Computer Communications Workshops (INFOCOM WKSHPS), IEEE Conference, p.614 – 618, 2011.

[5] David C. lee, Daniel 1. lough, Scott F. Midkiff, Nathaniel J. Davis IV, and Phillip E.Benchoff, "The Next Generation of the Internet:Aspects of the Internet Protocol Version 6" , Network, IEEE,Vol.12 , Issue 1,pp.28-33,1998.

[6] Anargyros Garyfalos and Kevin C. Almeroth, "A Flexible Overlay Architecture for Mobile IPv6 Multicast", Selected Areas in Communications, IEEE Journal, vol.23, Issue 11, pp.2194-2205, 2005.

[7] Seonggeun Ryu, Kyunghye Lee, Youngsong Mun, "Optimized fast handover scheme in Mobile IPv6 networks to support mobile users for cloud computing", The Journal of Supercomputing, vol.59, Issue 2, 2012.

[8] Ruay-Shiung Chang, Gao, J. ; Gruhn, V. ; Jingsha He ; Roussos, G. ; Wei-Tek Tsai "Mobile Cloud Computing Research - Issues, Challenges and Needs", Service Oriented System Engineering (SOSE), 2013 IEEE 7th International Symposium, pp.442-453,2013.

[9] Ren-Hung Hwang, Member, IEEE, Cheng-Ying Li, Chiung-Ying Wang, and Yuh-Shyan Chen, Member, IEEE, "Mobile IPv6-Based Ad Hoc Networks: Its Development and Application", Selected Areas in Communications, IEEE Journal, vol.23, Issue 11, 2005.

[10] Hongyan Li ; Coll. of Inf. Eng., Taiyuan Univ. of Technol., Taiyuan, China ; Xueying Zhang ; Jiaqi Fan, "The safety analysis of IPSec based on IPv6 protocol", Circuits,Communications and System (PACCS), 2010 Second Pacific-Asia Conference, vol.2, pp.35-38, 2010.

[11] Dequan Yang ; Sch. of Autom., Beijing Inst. of Technol., Beijing, China ; Xu Song ; Qiao Guo, "Security on IPv6", Advanced Computer Control (ICACC), 2010 2nd International Conference, vol.3, pp.323-326, 2010.

[12] Faigl, Z. ; Budapest Univ. of Technol. & Econ., Budapest ; Fazekas, P. ; Lindskog, S. ; Brunstrom, A., "Performance Analysis of IPsec in Mobile IPv6 Scenarios", Mobile and Wireless Communications Summit, 2007. 16th IST, pp.1-5, 2007.

[13] Michelle X. Gong, Scott F. Midkiff, Shiwen Mao, "A cross-layer approach to channel assignment in wireless ad hoc networks", Mobile Networks and Applications, vol.12, Issue 1, pp.43-56, 2007.

[14] Daniele Puccinelli, Emmanuel Sifakis, Martin Haenggi, "A Cross-Layer Approach to Energy Balancing in Wireless Sensor Networks", Networked Embedded Sensing and Control Lecture Notes in Control and Information Science, vol.331, pp.309-324, 2006.

[15] Kyunghye Lee, Seonggeun Ryu, Youngsong Mun, "An enhanced cross-layer fast handover scheme for mobile IPv6 in the IEEE 802.16e networks", The Journal of Supercomputing, vol.29, Issue 2, 2012.

[16] Eiman Alotaibi, Biswanath Mukherjee, "A survey on routing algorithms for wireless Ad-Hoc and mesh networks", Computer Networks, vol.56, Issue 2, pp.940-965, 2012.

[17] Azzedine Boukerchea, Begumhan Turgutb, Nevin Aydinc, Mohammad Z. Ahmadd, Ladislau Bölönid, Damla Turgutd, "Routing protocols in ad hoc networks: A survey", Computer Networks, vol.55, Issue 13, p.3032-3080, 2011.

[18] Shahzad Ali, Sajjad A. Madani, Atta ur Rehman Khan, Imran Ali Khan, "Routing Protocols for Mobile Sensor Networks: A Comparative Study", International Journal of Computer Systems Science & Engineering, vol 29, no 1, 2014.

[19] Azzedine Boukerche, Sheetal Vaidya, "A Performance Evaluation of a Dynamic Source Routing Discovery Optimization Protocol Using GPS System", Telecommunication Systems, vol.22, Issue 1-4, pp.337-354, 2003.

[20] Adam Macintosh, Mohammad Ghavami, Ming Fei Siyau, "Lightweight Local Area Network Dynamic Routing Protocol for MANET", International Journal of Soft Computing and Software Engineering [JSCSE], Vol. 2, No. 7, pp. 9-25, 2012.

[21] S. Basagni, I. Chlamtac and V. Syrotiuk, "A distance routing effect algorithm for mobility (DREAM)", Proc. of IEEE/ACM MOBICOM'98, pp. 76–84, 1998.