ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

A Survey on Various IP Mobility Solutions

Srivitha S Vijayan [1], Divya R.S [2]

P.G. Student, Department of Computer Engineering, Mar Baselios Engineering College, Kerala, India[1]

Associate Professor, Department of Computer Engineering, Mar Baselios Engineering College, Kerala, India[2]

ABSTRACT: The mobile workforce needs the ability to communicate with customers, partners, and fellow workers anywhere, anytime and have access to relevant business applications, tools to carryout business effectively. Enterprise mobility is about providing ubiquitous connectivity to the mobile user, independent of the devices and access technologies. Mobile IP allows a host device to be identified by a single IP address even though the device may move its physical point of attachment from one network to another. Regardless of movement between different networks, connectivity at the different points is achieved seamlessly without user intervention. Roaming from a wired network to a wireless or wide-area network is also done with ease. Mobile IP provides ubiquitous connectivity for users, whether they are within their enterprise networks or away from home. Mobile IP is part of both IPv4 and IPv6 standards.

KEYWORDS SMSL,IP,IPv4,IPv6,HIP,TCP,DHCP.

I. INTRODUCTION

Developing a safe and secure network infrastructure means integrating security into the foundation of the network. Efficient and intelligent use of bandwidth is paramount, particularly with the advent of video, mobility, and cloud technologies. It is also critical considering the surge in related one-to-many or many-to-many communication-based applications. Multicast helps to fulfil the requirement of such bandwidth-intensive applications with its inherent ability to replicate single stream when and where necessary. Applications across industries such as finance, enterprise, content-provider, entertainment, education, ISPs, and surveillance use multicast to optimize the profit-potential of resources with efficient and quality service offerings. Mobile IP intelligence is a suite of value-added technologies and features support more protocol interfaces than any other internetworking supplier in the industry. The IP routing protocols comprise the basics for delivery of high availability, scalability, and connectivity that enterprises and service providers alike require for today's business applications. A communications network forms the backbone of any successful organization. These networks transport a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. The bandwidth-intensive applications stretch network capabilities and resources, but also complement, add value, and enhance every business process. Networks must provide secure, predictable, measurable, and sometimes guaranteed services. Achieving the required Quality of Service (QoS) by managing the delay, delay variation (jitter), bandwidth, and packet loss parameters on a network becomes the secret to a successful end-to-end business solution. Thus, QoS is the set of techniques to manage network resources.

II. LITERATURE SURVEY ON DIFFERENT MOBILITY SOLUTIONS

During the last decade many mobility solutions have been proposed. Most of them Such as Mobile Internet Protocol, HIP, TCP-Migrate, SSL/TLS Resilient Connections, and nearly MPTCP require modifications on the legacy protocol stack. But deployment problems are seen in those environments. In Application Layer ROCKS and SIP manage this problem. Based on the category of solutions, our goal is to form the best solution for mobility protocols in the upper-layer into a unique, which is implemented in the mobile node's user space.

Paper is organized as follows.Section III to IX describes different mobility solutions for single homed mobile nodes. Finally, Section X presents conclusion.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

III. IP MOBILITY IN IPv4

Internet protocol version 4 permit routing of IP datagrams to mobile nodes in the Internet .Regardless of its current point of appointment to the Internet each mobile node will be always recognized by its home address. A mobile node is consisting of a care of address while it located away from its home, which gives information about its current point of appointment to the Internet. The protocol is needed for entering the care of address with a home agent. Through a tunnel home agent transmit datagrams destined for the mobile node to the care of address. Every datagram is transferred to the mobile node after reaching at the tunnel end. This protocol shows that node's IP address can recognizes the node's point of fitment to the Internet uniquely. In order to get the datagrams intended to the node It must be placed on the network by that IP address; else datagrams intended to the Node cannot be delivering. For a node to make different point of fitment without losing its facility to communicate, any one of the two following methods must be generally follow. Currently: At whatever time the point of fitment changes, the node need to change its IP address. Host specific routes need be transmitted through the fabric in the Internet routing. These two alternate are insupportable. When the location of the node changes, first makes it unfeasible for a node to retain transport and higher layer connections. The second has prominent and major scaling issues, mostly applicable to the rapid increment in sales of mobile computers. For considerate mobility of the node within the Internet there require a new scalable method. This protocol defines such a method which permits nodes to make different point of fitments to the Internet by unchanging their IP address. The link by where a mobile node is directly fitted to the Internet may sometimes be a wireless link. Contrasted to traditional wired networks this link may have a considerably lower bandwidth and higher error rate. Operation of Mobile IP version 4 are by standard IP routing, datagram to mobile node reaches on home network .Datagram is interrupted by home agent and is then tunnelled to the care of address. Datagram is then tunnelled and remitted to the mobile node. Standard IP routing dispatched each to its destination, for datagrams transmitted by the mobile node. But IPv4 have the following consequences. There can occur triangle routing which is defined as the routing inefficiency problem made by the home agent, correspondent host, and the foreign agent. The most important problem of Mobile IP is the security risks. One has to bother about wrong care of addresses, except the traditional security risks with IP. The other problem related to the security is how to make Mobile IP already exist with the security aspect coming in use within the Internet.

IV. IP MOBILITY IN IPv6

The Internet works based on IP version 4 makes so many issues. IPv4 changes have expanded the life of the current Internet that makes new issues and need consistent above network administration. IP version 6 has been implemented to assist these expansions without making more issues. IPv6 is an improved version of IPv4. IPv6 has different extended headers, which includes Routing header and Destination options header, that supports mobility. Also, it made mechanisms for Stateless Address Auto configuration and Neighbour Discovery. To improve Internet security IPv6 have strong encryption authentication. A mobile node registers any one of its bindings with a router in its home subnet, requesting this router to perform as the home agent for the mobile node if away from home. The primary care-of address of mobile node's is the care-of address binding registered with its home agent, and home registration is the mobile node's home agent keeps this entry in its Binding Cache up to lifetime expires. Since in its Binding Cache there is a home registration entry, to interrupt, the home agent uses proxy Neighbour Discovery. When the location of the node changes , first makes it unfeasible for a node to retain transport and higher layer connections. The second has prominent and major scaling issues, mostly applicable to the rapid increment in sales of mobile computers. For considerate mobility of the node within the Internet there require a new scalable method. This protocol defines such a method which permits nodes to make different point of fitment to the Internet by unchanging their IP address. The link by where a mobile node is directly fitted to the Internet may sometimes be a wireless link. Contrasted to traditional wired networks this link may have a considerably lower bandwidth and higher error rate. To enable a mobile node's home agent and correspondent nodes grasp and cache the mobile node's binding, mobile IPv6 establishes two new IPv6 Destination options. A mobile node must transmit a Binding Update option holding that care-of address to its home

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

agent after computing a new care-of address and any correspondent nodes that have an expired care-of address for the mobile node in their Binding Cache. If an acknowledgement was required in the Binding Update, arrival of a Binding Update needs to be acknowledged by a Binding Acknowledgement option. The Internet Protocol version 6 has the following consequences such that IPv6 Deployment is a big question for internet management groups, stake holders and service providers.

V. MOBILITY IN HOST IDENTITY PROTOCOL

The Host Identity Protocol (HIP) is an architecture based on internet working and Its protocols, developed by IETF in 1999 and obtained first consistent version in 2007. HIP is formed on the original Internet architecture by joining a name space used between the IP layer and the transport protocols. This new name space contains cryptographic identifiers, as a result of that executing the so-called identifier/locator split. In this new architecture, the new identifiers are implemented in naming application level end-points, restoring the initial identification role of IP addresses in applications, TCP con-nections, sockets, and UDP-based transmit and obtain system calls. IPv4 and IPv6 addresses are implemented for topological locations in the network. HIP can be exploited such that no modifications are needed in routers or applications. The HIP routing and identification of HIP packet can be completely districted from each other. A host accepting a HIP control packet can authenticate its origin by authenticating the packet signature; otherwise the two endpoints of an active HIP as-sociation can quietly authenticate the message authentication code. A host accepting a data packet can certainly find out the transmitter through a three step process: firstly it detects an ESP Security Association based on the Security Parameter Index carried in the packet. In the second step, if needed it authenticate packet integrity and then decrypts the packet. Last in the third step, it setting into the packet the source and destination HITs, as stored within the ESP BEET mode SA. [5]. When handover are done in the break-before make manner, all connectivity can be lost for some time. While the handover can be done even without any packet, enriching the handover performance significantly, HIP supports make-before-break style handover. The Host Identification Protocol also have the following consequences Universal connectivity loss. For mobility and multi-homing the support is poor. Multi cast problem is there. Unwanted traffic is there. HIP have lack of authentication, privacy and accountability.

VI. MOBILITY IN TCP MIGRATE

When handovers are happened in the break-before make manner, all connectivity can be off track for some time. While the handover happens even without any packet, enriching the handover performance substantially HIP allow to track host location this method is executed on the basis of an end-to-end architecture the Domain Name System dynamic updates for Internet host mobility. To allow an entrenched connections to seamlessly contract a change in endpoint IP addresses without any third party, available TCP connection is conserved using efficient and secure migration of connection. The migration of TCP connection implements a set of Migrate options and gives a pure end-system substitute to routing-based means like Mobile IP. This architecture is reliable and using secure DNS update protocol the name updates are executed . Fixed Internet applications and hosts were not modified and only the elementary IP substrate should change is the principle behind Mobile IP .This architecture didn't need any changes to the unicast IP substrate, alternatively changing applications and transport protocols at the end hosts. TCP migrate latencies handover times are ruled by the communicating peers based on round-trip time. There are three important elements in the end-system mobility architecture, there are addressing, mobile host location, and connection migration. Eliminating the use for an extra home-agent to the broker packet routing , mobile host can distinct control over its mobility mode. When mobile host changes network location the DNS gives a service in the host location ,and then the control is controlled by the communicating peers, prompted on the mobile host. The communicating peers should safely overcome any modification in the network-layer IP address underlined and recommence communication.

The end-to-end TCP option to assist the secure moving of an entrenched TCP connection over an change in the IP address. A TCP peer can resume the open connection and again activate that from any another IP address, explicit to an

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

application that predict not interrupted definitive communication with the peer. During initial connection initiation, reliability is obtained through the use of a connection identifier it is assured by a shared secret key overcome through the Elliptic Curve Diffie-Hellman key exchange. To obtain seamless mobility can be executed in UDP-based protocols such as the RTP for those protocols as well. [11] A mobile host again starts the formerly initiated TCP connection from a new address by transmitting a special Migrate SYN packet that includes the token identifying the former connection. A moved connection retains the same state and control block containing the sequence number space. This also verifies that SACK to works correctly. The initial SYN exchange persists after connection migration. Once a moving SYN has been sent, the token is known by any hosts and DoS attacks could be established by transmitting SYNs with correct tokens. If a mobile host contains a new SYN, when the last connection token can be implemented is quite small only until the new three-way handshake is achieved.[11] The consequences of using TCP migrate protocols are disconnectivity of host is not supported. Also simultaneously Both peers cannot move and TCP migrate protocols can be used with any UDP-based protocols by less plight.

VII. MOBILITY IN SESSION INITIATION PROTOCOL

The Session Initiation Protocol is an application-layer protocol which is used for creating and tearing down multimedia sessions that can be either unicast or multicast. It is standardized within the IETF for multicast conferences and Internet telephone calls. Components in SIP are proxy servers, user agents and redirect servers. SIP transaction has a distinctive call identifier that recognizes the session. SIP defines a number of methods and responses to methods shows success or failure. If the session required to be modified, the call identifier is defined in the initial request, to show the modification of a subsisting session. The mobility support in SIP is executed. The mobile host has both mobile IP, and a SIP client. The host has a wireless interface, and uses DHCP for IP address. With the SIP mobility and mobile IP Together it is preferable to comprise a lower layer support in order to have a complete solution. SIP assists personal mobility, the step from personal mobility to IP mobility support is generally the roaming frequency, and that a user can make different location during a traffic flow. Therefore, in order to assist IP mobility, require to add the facility to move while a session is active. It is presumed that the mobile host belongs to a home network, on which there is a SIP server which get registrations from the mobile host every time it alters the location. This is likely to home agent registration in Mobile IP. The mobile host does not required to have a statically obtained IP address on the home network. When the correspondent host transmits an INVITE to the mobile host, the again direct to server has current information about the mobile host location and redirects the INVITE there. [12] TCP connections are not supported in SIP mobility, best solution would be appeal SIP mobility for real time communication, and Mobile IP for TCP connections. If we permit the mobile host to allow when to use its home address or care-of address. When initiating TCP connections, it will use the home address and the traffic will routed by the home agent and when transmitting RTP streams and it will apply the care-of address. The TCP connection applies route optimization. The consequences in SIP includes for the data transmission dynamically allocated ports needed. It will be contacted to change or terminate the session, if the original session participant has to persist in the session.

VIII. MOBILITY IN RELIABLE SOCKETS

Reliable sockets (rocks) and Reliable packets (racks) are the two new systems in which both give transparent network connection mobility to ordinary applications by only user level mechanisms. They can find network connection failures, including those caused by link failures, IP address modification, process migration and large periods of distortion, within seconds of their happening. When connectivity is restored, they can again obtain the cracked connections without any reduction of in-flight data. When an application inserting any one of these systems a new connection is executed, it securely the remote peer for the existence of a rocks or racks permitted socket, and get reverted to normal functionality of socket. Then delineate to be ready-to-use by ordinary users, without making kernel

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

modifications, the two system can be worked without compiling again or linking again implemented binary and rocks can be installed for non-privileged users. The way rocks and racks track communication is the major dissimilarity between them. Rocks work based on the library between the operating system and application code. While expanding the performance of functions to hide failure of connection from the application, the library transport the sockets API to the application and allowing it to be explicitly released into ordinary applications. Racks are worked on a different user-level process which redirect the flow of selected packets using an advanced kernel-level packet filter ; functionality currently involve in the FreeBSD divert sockets in the packet filters and also in the Linux net filter. Racks don't need code to be place in any processes which utilize them. Both methods exhibit transparent intensification of network communication functionality in user-space without need any changes in the kernel. Rocks are executed between the kernel and application process at two ends of a TCP connection. Then the library sends the sockets API to the application code to provide it to be explicitly deposited in the ordinary applications. The library also sends the rocks extended API (RE-API), which allows mobile-aware applications to put policies for the behaviour of the rocks and to physically manage some of its methods. A rocks are defined on three states they are CLOSED, CONNECTED, and SUSPENDED. The above states equivalent to rocks nature that alter the process, doesn't the internal state of TCP socket preserved in the kernel. A rocks start process when it is in CLOSED state. To achieve a reliable socket connection, the application code creates the usual sequence of sockets API calls to make a TCP connection. [3] The consequences of using reliable sockets are during the period of disconnection if the other end moved then cannot accomplish a new connection. A firewall is used to block from introducing a new connection. A NAT device is pretended by the last known address of the peer.

IX. A SESSION BASED MOBILE ARCHITECTURE

Most of the above mentioned methods have one or the other drawbacks with respect to the required specifications for IP mobility. So the proposed system is meant to overcome these drawbacks by incorporating techniques to implement all of the above in a single solution. The proposed system handle mobility using a non-intrusive communication session with a TCP/IP stack, named it SMSL, which is appropriate for applications that need the establishment of a secure connection, reliable end-to-end transmission, and tolerance to disruptions/disconnections generated by host mobility. SMSL is concentrated on TCP-based communications because TCP is widely allows the end-to-end reliable protocol on the Internet. The term disruption is defined as each and every event related to the loss of IP connectivity, which intercepts obtaining access to the Internet. Sessions in SMSL overcome parameters during the establishment of communication between mobile peers, in addition to granting services to constantly manage the application state in the event of broken connections. A GNU/Linux implementation sends SMSL as a general-purpose API to permit for the formation of mobility aware applications. Not like other session-based architectures, proposed system is inventive in that it collect different mobility methods into a single object, which is a lightweight and efficient methods. The proposed session method gives transparent services: tracking of mobile nodes with the support of a Distributed Hash Table (DHT),which is allowed to recover location registers stored under distinctive mobile host identifiers; detection of disconnection, for link disruption and re-establishment; session suspension by blocking transmission whenever a link and session are unready for use; again opening suspended sessions by synchronizing transmitter and receiver with current session information on a new TCP connection. [1] To obtain seamless handovers, the proposed SMSL aims to reduce the time elapsed during events under its control: We begin from the hypothesis that distributed applications can cause communication failures. There are detection methods in the Sockets API to know the absence of a link. Similar to node authentication, an application could handle mobility associated events, such as timeouts, broken connections and re-establishment, losses of unconfirmed data, location independent identification, and location services. Session abstraction is useful in restricting the scope and duration of a connection while keeping the TCP/IP stack intact. Concerning the wide range of applications and communication scenarios that occurs, on the one hand, there is the require for efficient solutions that permit for less disconnection time to allow seamless mobility. On the other hand, due to mobile node drawbacks there is a necessity for low-cost solutions that are simply to exploit and sustain and transparent in the TCP/IP stack. Session abstraction with critical data structures to creates disruption tolerance. The

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

purpose of a DHT to support the Location Management of mobile peers. The trigger management allowed identifying disruptions.

Parameters	MIP	HIP	TCP-Migrate	SIP	ROCKS	SMSL
Operation Layer	L3	L4	L4	L5	L5	L5
Implementation	Kernel space	Kernel space	Kernel space	User space	User space	User space
Host Identifier	-	HIT (128 bits)	Token (32 bits)	URI	Connection ID	h_{id} (160 bits)
Infrastructure dependency	Home Agent (HA), Foreign Agent (FA)	RVS (HLR)	DDNS (HLR)	Redirect, Proxy, Registrar servers.	DNS (HLR)	DHT (HLR)
Security support	Location registration authentication	IPSec	ECDH	User level authentication	Diffie-Hellman	RFC 6287
Modification on the TCP/IP stack	yes	yes	yes	no	no	no
Deployment cost	high	high	high	medium	low	low
Transparency	native	native	native	no native support	Reliable Packet (RACK) filtering	syscall interception LD_PRELOAD
Reliability	Above layer (TCP)	Above layer (TCP)	Native with TCP modifications	no native support	In-flight send and receive buffers	Ancillary session send buffer
IEEE 802.21 support	no native support	no native support	no native support	no native support	no native support	MIH Link Up and Link Down
Handover latency	> 1 s simulation, ~ 10 s experiment	< 1 s simulation	< 1 s simulation	> 2 s simulation	< 2 s experiment	< 1 s experiment

Fig. 1. Comparison Among Related Mobility Protocols for Single-Homed Mobile Nodes

X. CONCLUSION

All the technique proposed is to be implemented which shows several problems with the existing techniques. The proposed system defines the full concept of a Session-based Mobile Socket Layer with the goal of granting communication disruption tolerance for legacy applications on the mobile Internet. There are many existing IP mobility solutions, SMSL is a user space implementation based protocol that gives the easy deployment and maintenance of a simple software component while maintaining the TCP/IP protocol stack intact. The middleware granted by the mobile socket layer architecture permits for the incorporation of new functionalities with single control modules. Because it is capable of re-opening suspended sessions in dozens of milliseconds with consistency and reliability and without loss, SMSL shows good performance in terms of per-link utilization during handover and low utilization overhead for single-homed mobile nodes.

REFERENCES

[1] Bruno Yuji Lino Kimura, Hlio Crestana Guardia, and Edson dos Santos Moreira," A Session-Based Mobile Socket Layer for Disruption Toler-ance on the Internet" IEEE TRANSACTIONS ON MOBILE COMPUT-ING , vol. 13, no. 8,pp. 1668- 1680 August 2014.
[2] B.Y.L Kimura, H.C.Guardia, and E.S.Moreira, Disruption tolerant sessions for seamless mobility, in Proc. IEEE WCNC, Shanghai, China, Apr. 2012, pp. 24122417.
[3] B. Y. L. Kimura, R. S. Yokoyama, H. C. Guardia, and E. S. Moreira, Secure connection re-establishment for session-based IP mobility, in Proc. 2nd Brazilian Conf. CBSEC, Campinas, Brazil, May 2012, pp. 5863.
[4] P. A. Shah, M. Yousaf, A. Qayyum, and H. B. Hasbullah, Performance comparison of end-to-end mobility management protocols for TCP, J. Netw. Comput. Appl., vol.35, no. 6, pp. 16571673, 2012.
[5] J. Ahrenholz, Host identity protocol distributed hash table interface, RFC 6537, Feb. 2012.
[6] M. Yousaf, A. Qayyum, and S. A. Malik, An architecture for exploiting multihoming in mobile devices for vertical handovers and bandwidth aggregation, Wireless Personal Commun., vol. 66, no. 1, pp. 5779, 2012.
[7] S. Cespedes, X. Shen, and C. Lazo, IP mobility management for vehicular communication networks: Challenges and solutions, IEEE Commun. Mag., vol. 49, no. 5, pp.187194, May 2011.
[8] A.Ford,C Raiciu, M. Handley, S.Barre,and J. Iyengar, Architectural guidelines for multipath TCP development, RFC 6182, Mar. 2011.
[9] D. Johnson, C. Perkins, and J. Arkko, Mobility support in IPv6, RFC 6275, Jul. 2011.
[10] C. E. Perkins, IP Mobility Support for IPv4, revised, RFC 5944,Nov. 2010.
[11] B. Y. L. Kimura, R. S. Yokoyama, R. R. F. Lopes, H. C. Guardia, and E. S. Moreira, Prototyping applications to handle connection disruptions in end-to- end Host Mobility, in Proc. 7th IEEE WONS, Kranjska Gora, Slovenia, Feb. 2010, pp. 18.
[12] Elin Wedlund,Henning Schulzrinne, Mobility Support using SIP Nov. 2010.