International Journal of the Physical Sciences Vol. 6(12), pp. 2958-2964, 18 June, 2011
Available online at http://www.academicjournals.org/IJPS
DOI: 10.5897/IJPS11.628
ISSN 1992 - 1950 ©2011 Academic Journals

Full Length Research Paper

A mathematical model to determine the maximum end-to-end delay bound on label switched path for real time applications over mobile IPv6

Reza Malekian* and Abdul Hanan Abdullah

Faculty of Computer Science and Information Systems, University Technology Malaysia, Johor, Malaysia.

Accepted 17 May, 2011

The real time applications have driven the demand for increasing and guaranteed bandwidth requirements in the network. Due to the mobility feature within a MN, mobile networks need a more sophisticated mechanism for quality of service provision. Beside, custom routing methods in a Mobile IPv6 network deliver a packet via specific tunnel this causes intermediate routers do not recognize content of a control packet due to adding headers in IPv6-in-IPv6 encapsulation. In this paper, we propose a mathematical model by using an effective envelope approach to traffic engineering and determine bound of end-to-end delay between MN and correspondent node according to ROMA solution in mobile IPv6 networks. According to this method, every transmitted flow over label switched path should have an end to end delay less than estimated end-to-end delay; otherwise, they will be ignored. This causes an improvement of the network performance and increase achievable link utilization and ultimately increasing quality of services over mobile IPv6 networks. The proposed mathematical model is applicable on label switched path which is a result of ROMA approach to quality of service provision over mobile IPv6 networks.

Key words: Mobile IPv6, quality of service, traffic engineering, end to end delay.

INTRODUCTION

Firstly, in this paper, we discus about quality of service (QoS) problem over Mobile IPv6 networks and then we introduce ROMA approach for solving this problem. Finally, we present our mathematical model to traffic engineering over label switched path in ROMA approach.

Custom routing methods in Mobile IPv6 networks for routing IPv6 packets from correspondence node (CN) to mobile node (MN) and vice versa are bi-directional tunneling and routing optimization (RO).

In bi-directional tunneling mode, according to Le et al. (2010), when CN sends packets to MN, it sets destination address to MN' home address in the IPv6 header of packets and these packets are routed via IPv6 routing methods. Then, CN intercepts and tunnels them to MN. Beside this, in reverse side, MN sends packets in reverse tunnel to Home Agent (HA) and HA uses regular IPv6 routing to route these packets to CN. The bi-directional tunnel mode is illustrated in Figure 1.

Another routing method in Mobile IPv6 is RO (Le et al., 2010). RO is a technique that MN registers its binding on HA and also CN and enables CN to address packets to a mobile's current Care of Address (CoA). In MIPv6, each IPv6 terminals and HA have binding table to support RO and maps the mobiles' home addresses to their CoAs. Whenever a CN node sends a packet to MN, it first checks its binding cache to search and find an entry to MN. If a binding cache entry is found, the CN sends packets to mobile's COA directly, otherwise, it sends packet to mobile's home address. Then, HA discard packets and send them via tunnel to MN. Next, MN lets CN knows its current location by sending binding update. Finally, CN and MN can communicate directly.

As shown in Figure 2, although, RO reduces the number of packets that have to experience tunneling but it uses tunneling to sending initial packets. On the other hand, RO is facing to nested tunneling problem (Lim et

*Corresponding author. E-mail: reza.malekian@yahoo.com

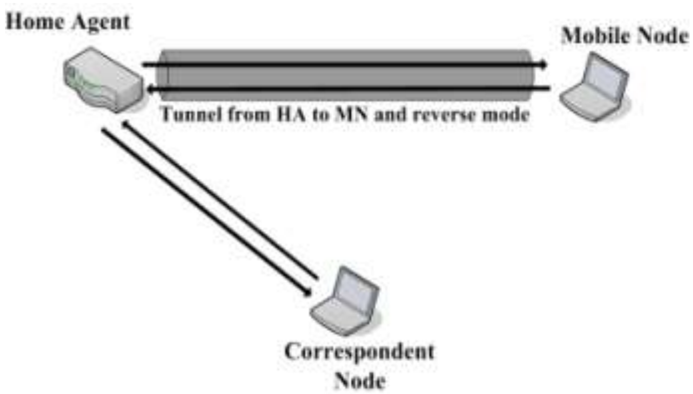

Figure 1. Bi-directional tunneling.

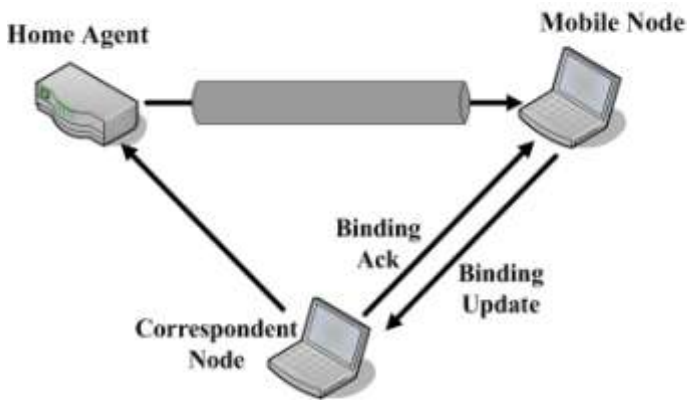

Figure 2. Routing Optimization in Mobile IP version 6.

al., 2009).

The encapsulating process could be repeated by transmitted network node or routers and with each iteration, packet size and time to live grow.

Related works

The growing demand for real-time applications in mobile networks has resulted in more and more active researches to be done on scalability, compatibility packet routing with minimal changes to the network infrastructure. Some improvements have been suggested to solving tunneling problem for real-time applications. Le et al. (2007) proposed an end-to-end tunneling extension to mobile IPv6 with lower packet routing overhead. Although authors in this approach were successful to decrees bidirectional routing overhead, while, it is not efficient to minimize end-to-end delay. Proposed method in (Le et al., 2010) keeps minimal changes to network infrastructure. The authors introduce an extension to mobile IPv6 for transit packets via tunnel. With this approach, packets rate routed through end-to-end tunneling between the mobile node and the correspondence

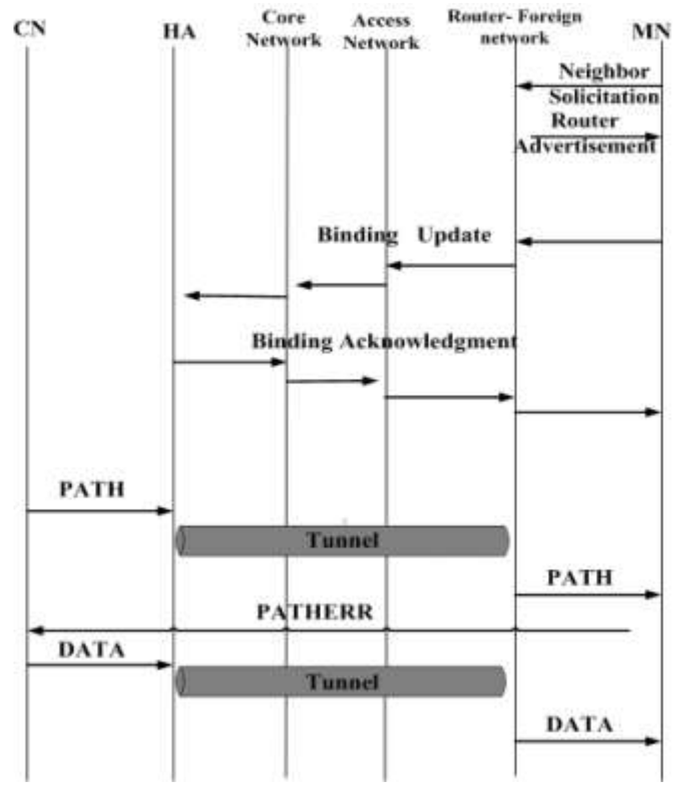

Figure 3. Resource reservation failure based on RSVP in Mobile IPv6.

node, while, this solution is not efficient to decrees end-to-end delay.

Vogt et al. (2005) proposed an optimized mobility signaling to decrees long latency binding update especially for delay-sensitive applications. Although this solution acts efficiently but it needs to change handoff methods (Malekian et al., 2008) according to modified mobility signaling. Belhoul et al. (2009) proposed a mobility-aware resource reservation protocol in which mobility and QoS signaling are performed as a single functional block.

The idea in this proposal is to convey mobility information by using newly defined RSVP objects embedded in existing RSVP signaling.

QoS improvement, that is 12.5% in Hierarchical mobile IPv6 and no improvement in Fast handoffs for Mobile IPv6, is very trivial by comparing simulation results and signaling and infrastructure modifications in networks.

The problem of resource reservation in mobile IP

To understanding the reservation resource problem in Mobile IP networks, we consider a scenario that is exhibited in Figure 3. As there are no foreign agents in foreign networks in Mobile IPv6, MN uses from the neighbor discovery protocol (Beck et al., 2007) and finds its current location by addressing auto-configuration. The main task of the foreign agent is to help MN to find its care of address. It enables MN receives a packet from a correspondent node directly or indirectly. It is also useful for Mobile IP hand offs (Malekian et al., 2008). On the other hand; a neighbor discovery protocol does this task in Mobile IPv6. MN can configure its care of address by using neighbor discovery protocol.

Neighbor discovery enables a terminal to discover new routers and determine if a router is reachable. An IPv6 router broadcasts the router advertisement message (Koodi et al., 2007) on a local network periodically. This message carries some information such as the IPv6 address of the router and network prefix. When the MN receives this message it can compare the information against the last one it has received and can construct its care of address (ithat is, auto-configuration) based on the network prefix and also detect whether it has moved to a new network or if it has stayed in the current network. Furthermore, it can detect the IPv6 address of the router and determines whether the router is still reachable or not.

From Figure 3, firstly the MN sends a neighbor solicitation message for asking from the new network if there is any reachable router and if there is, it should introduce the specification. In a real network when the MN is entering the new network, it receives a router advertisement message periodically. When a MN receives this message it can find out its required details. If a MN did not receive this message after a few times, it distributes the neighbor solicitation message. By broadcasting this message, the MN asks from the new network for a reachable router specification.

Whenever a MN receives router advertisement message it can detect its current address. The MN then reports the current address to the home agent by sending a binding update message.

The home agent approves it and determines the current address of the MN by sending a binding acknowledgment message. The next step is where the correspondent node sends a PATH message. As shown in Figure 3, a PATH message is forwarded through the tunnel. This message will then be encapsulated and the router cannot recognize a PATH message because this message was encapsulated for travel into the tunnel. Finally the correspondent node receives PATHERR. Path error message indicates that intermediate routers were not able to detect PATH message and therefore, can not provide a level of QoS requirements for next packets (Bulhoul et al., 2008).

The problem will be most important for real-time traffics, or streams of data with high priority because these type of application certainly need reserved resource and guaranteed a high level of QoS.

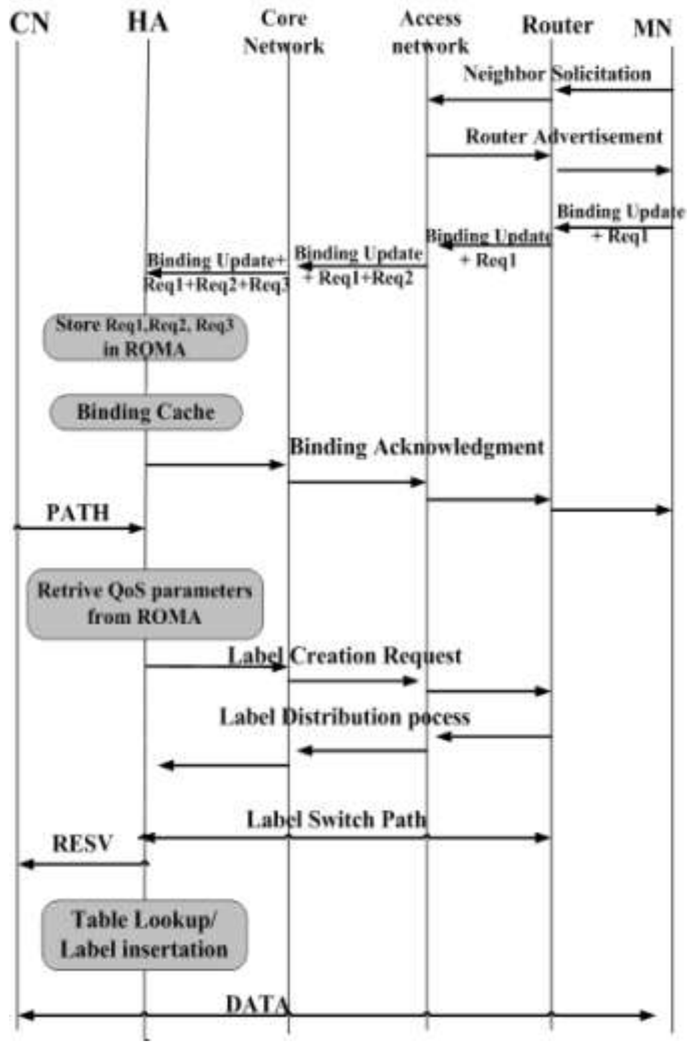

Figure 4. ROMA Implementation on mobile IP network.

METHODS

By collecting QoS parameters from source to destination and modification of existing signaling, this section explains how ROMA solution (Malekian et al., 2011b) acts on mobile IP network and intermediate routers recognize resource reservation request? As mentioned before, the main problem for QoS provision in bi-directional tunneling is related to tunneling and hides QoS parameters from intermediate routers along tunnel. To overcome this problem we suggest an approach to cross layer scheme (Malekian et al., 2011 a). Furthermore, we use information from existing signaling to avoid the introduction of new signaling and also to increase new overload. Moreover, a diagram is used to store and retrieve QoS parameters which collect parameters from modified signaling.

MPLS components (Yi et al., 2009) are used to tunnel redundancy. As shown in Figure 4, when the MN sends “Binding update”, this message piggybacks the application’s QoS requirements (Malekian et al., 2011a). This message passes via the access and core network and collects QoS requirements of access, core networks finally receives it. HA collects QoS parameters and stores them in ROMA diagram, then updates its binding cache and insert new CoA. Finally, HA sends a Binding Acknowledgment message to confirm new CoA.

Thereafter the CN sends a resource reservation request (PATH), HA retrieves QoS parameters from ROMA diagram (Malekian et al., 2011a). The QoS requirements which are collected and stored in ROMA diagram is useful to make same labels on a Forwarding equivalent class (FEC). In the next step, HA sends a label creation request to the MN.

That means before traffic begins the HA creates label and decides to bind labels to a specific FEC and builds its table. Then, foreign MN's router sends Label distribution protocol (LDP) to initiate the distribution of labels and label/FEC binding (Mellouk et al., 2008).

Then, label switched path (LSP) between HA and MN's router established. This can guarantee resource reservation over this path. So, CN receives RESV message. HA as (Label Edge Router) LER uses a label information binding (LIB) table to find the next hop and insert a label for the specific FEC. Finally, data can be transmitted on guaranteed QoS path.

Traffic engineering on MPLS-LSP based on effective envelope

Here, we propose a mathematical model to determine maximum bound of end-to-end delay based on effective envelope approach (Boorstyn et al., 2000). This model is applicable on established LSP between MN and CN. In this model individual flows aggregated and then aggregated traffic is inserted into a buffer and a scheduler determines the order of traffic on output link. We use first in-first out scheduling algorithm for scheduling traffic in scheduler in this paper. It is possible for using other schedulers, for example, earliest deadline first, last in-first out.

A model for QoS provisioning not only has to take into account the conformance of guaranteed bounds on services, it also should consider factors involving the scalability of the deployed QoS solution. By allowing a fraction of traffic to violate its QoS guarantees we assume that,

Probability {traffic violating QoS guarantees} < ε (1)

where ε is the maximum probability of QoS violations.

The arrival of packets is considered to be a random process in which a set of *C* packets that consist of *q* classes are allowed into the network.

Consider *Cq* to be the subsets of packets from class *q* and the random variable $A_i(t_1,t_2)$ to represent the arrival traffic from flow j in the time interval (t_1,t_2) . Then, considering A_{Cq} to denote the aggregate arrivals from the set *C* corresponding to the class *q,* we have the following relation,

$$A_{Cq} = \sum_{j \in C_q} A_j(t, t+\tau) \tag{2}$$

We assume that a traffic flows are characterized as follows:

a) Traffic arrivals A_{cq} are regulated by a deterministic sub additive envelope A^*_{cq} as,

$$A_{cq}(t,t+\tau) \le A^*_{cq}(\tau) \qquad \forall t \ge 0, \forall \tau \ge 0. \tag{3}$$

b) The A_{cq} are stationary random variables, that is,

$$\Pr[A_{cq}(t,t+\tau) \le x] = \Pr[A_{cq}(t',t'+\tau) \le x] \tag{4}$$

The input arrival can be considered as following equation:

$$A_{cq}(\tau) = \sigma_{cq} + P_{cq}\tau \tag{5}$$

The determination of upper bounds on reserved capacity at each node along a path for each class is based upon the concept of an effective envelope. A local effective envelope for $Acq(t,t+\tau)$ is a function $G_{cq}(0;\varepsilon)$ (Boorstyn et al., 2000; Liebeherr et al., 2000) which satisfies the inequality:

$$\Pr[A_{Cq}(t,t+\tau) \le G_{Cq}(\tau;\varepsilon)] \ge 1-\varepsilon \quad \forall t, \tau \ge 0 \tag{6}$$

In other word, a local effective envelope provides a bound for the aggregate arrivals $A_{cq}(t,t+\tau)$ for any specific time arrival of length τ .

$$G_{cq}(\tau;\varepsilon) = N \min(x, A^*_{cq}(\tau)) \ \forall \tau \ge 0. \tag{7}$$

Where,

$$A^*_{cq}(\tau) = \min\{P_{cq}\tau, \sigma_{cq} + p_{cq}\tau\} \tag{8}$$

It is clear that $P_{cq} \ge p_{cq}$ where P_{cq} is the peak traffic rate, p_{cq} is the average traffic rate, and σ_{cq} is a burst size parameter

.

$$p_{cq} = \lim_{\tau \to \infty} \frac{A_{cq}(t,t+\tau)}{\tau} \tag{9}$$

We define $\hat{\tau}$ as a function of class q at time t as follows:

$$\hat{\tau} = \inf\{x \ge 0 \mid A^{q,t}(t-x,t) \le x\} \tag{10}$$

In time interval [t- $\hat{\tau}$, t) the scheduler is continuously transmitting traffic. Beside, class q arrival at time t will leave the scheduler at time $t+\sigma$ if $\sigma \ge 0$

$$\sigma = \inf\{\tau_{out} \mid A^{q,t}(t-\hat{\tau}, t+\tau_{out}) \le \hat{\tau} + \tau_{out}\} \tag{11}$$

Class q arrival does not violate its delay bound d_q if and only if $\forall \hat{\tau}\, \exists \tau_{out} \le d_q$ that is,

$$\{A^{q,t}(t-\hat{\tau}, t+\tau_{out}) \le \hat{\tau} + \tau_{out}\} \tag{12}$$

The arrival from class q at time t does not have a violation if d_{cq} is selected such that

$$\sup_{\hat{\tau}}\{\sum A^{q,t}(t-\hat{\tau}, t+d_q)\ \} \le d_q \tag{13}$$

The probability that the arrival from time t experience a deadline violation is less than ε if d_q is selected such that

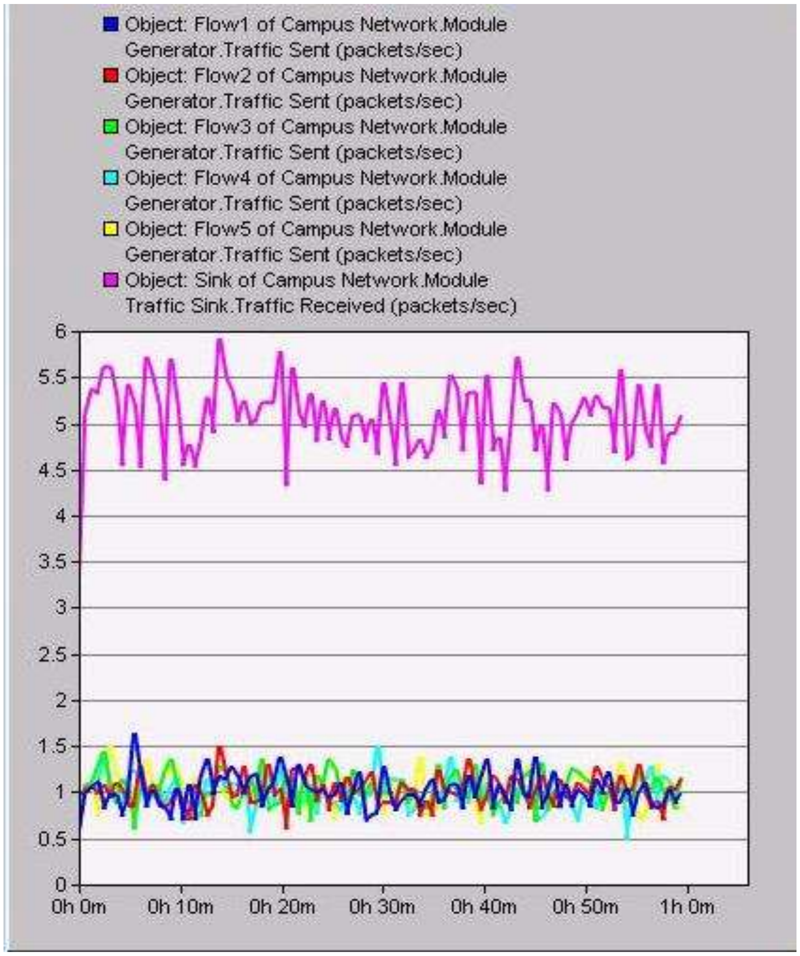

Figure 5. Sending and receiving traffic (Mbps) - Horizontal axis indicates the time in minutes, Vertical axis indicates sending and receiving packets (Mbps).

$$\left[\Pr\left\{\sup_{\tau>0}\sum A_{cq}(t-\hat{\tau},t+\overline{\tau})-\hat{\tau}\right\}\leq d_q\right]\geq 1-\varepsilon \quad -\hat{\tau}\leq\overline{\tau}\leq d_q \qquad (14)$$

Using a finite buffer of size *Bmq* at each node m for class *q*, the arrivals to a full buffer will be dropped while the arrivals that do get into the buffer will be served at a minimal rate denoted by *Cmq*. If we assume that the delay bounds at node *m* for class *q* is denoted by *dmq*, the problem of QoS provisioning results in the allocation of the network capacity *Cmq* which would be the smallest number satisfying the following inequality:

$$\sup_{\tau>0}(G_{mq}(\tau,\varepsilon)-c_{mq}\tau)\leq c_{mq}d_{mq} \qquad (15)$$

$$B_{mq}=c_{mq}d_{mq} \qquad (16)$$

Furthermore, the rate at which traffic would be dropped at node m due to a full buffer is bounded by Liebeherr et al. (2000):

$$\sum\varepsilon.\sup_{\tau>0}\{A^{*}_{Cmq}(\tau)-G_{mq}(\tau)\} \qquad (17)$$

While it is possible to deduce the statistical bounds on end-to-end delay and packet drop rates for packets of class q along a path p based on the bounds from Equations (4) through to (17), a deterministic bound (Rabbat et al., 2000) on these metrics are more informative and are presented below. Assuming a link capacity of *Lci* at node i along a path *P* consisting of *n* nodes with *Lmax* being the maximum transmission unit along the path with *propi* and *r* being the propagation delay at node *i* and the requested bandwidth respectively, we have the following deterministic bound for end to end delay:

$$End-to-End\ Delay_{\max}=\left(\frac{\delta+n.L_{\max}}{r}\right)+\sum_{i=1}^{n}\left(\frac{L_{\max}}{Lc_i}+prop_i\right) \qquad (18)$$

RESULTS AND DISCUSSION

Simulations are conducted using OPNET14.5 by considering the concepts of effective envelope. We consider different numbers of flows, (Figure 5), and generate packets with large sizes and distribute them with exponential function (in other words they are real-time application).

Then, flows are aggregated and aggregated traffic

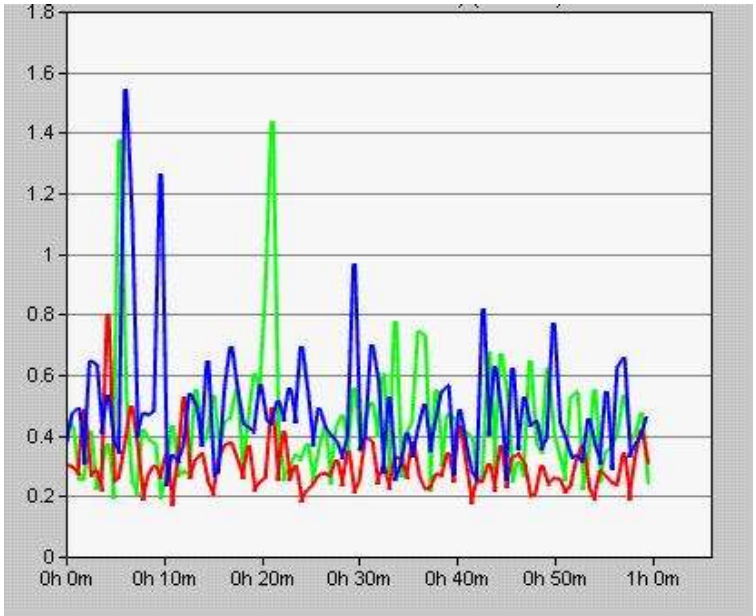

Figure 6. Maximum end to end delay for 5, 7, 10 flows. Red: 5 flows, Blue: 7 flows, Green: 10 flows.

controlled by leaky buckets. The simulation period is 60 min. In Figure 6, the horizontal axis indicates the time in which the mobile node are communicating with CN node in terms of minutes and vertical axis indicates the maximum end to end delay in terms of seconds.

We compare the number of flows with statistical QoS guarantees that can be admitted with effective envelope approach, and then we can reach maximum end to end delay to guarantee QoS in mobile IP networks according to effective envelop solution. We simulate our solution for maximum 10 flows as shown in Figure 6. According to Equation 1 and concept of statistical service, effective envelope solution allows a fraction of traffic to violate its QoS guarantees and end to end delay bound, therefore, maximum acceptable end to end delay in Figure 6 that could reach QoS guarantee is less than 0.8 s, as we did it just for single path. In other words, QoS can be guarantee when flows have a maximum end to end delay 0.8 s.

Ultimately, we obtain average end-to-end delay with running simulation in multiple times. As this figure shows maximum end-t-end delay is approximately 0.8 s.

Conclusions

Our contributions in this paper can be summarized as follow:

To model traffic engineering of the MPLS LSP that is, between MN and CNs for aggregated traffic from different correspondent nodes and to calculate maximum bound of end-to-end delay. This bound indicates that, a flow with end to end delay more than estimated bound will be ignored by network.

In this paper, we have proposed a mathematical model to determine maximum bound of end-to-end delay based on effective envelope approach. These model uses effective envelop solution which is proposed by (Boorstyn et al., 2000; Liebeherr et al., 2000; Rabbat et al., 2000). According to our proposed method, every transmitted flow over LSP path should have an end to end delay less than estimated end-to-end delay in this paper; otherwise, they will be ignored.

By nature of statistical services, this helps for improvement of the network performance and increase achievable link utilization.

Mathemathical model to determine the maximum end to end delay on LSP path considering several items such as link transmission rate, propagation delay, buffer size at each node, and maximum transmission unit along the path.

Then, a numerical evaluation is done by using OPNET 14.5 and comparing different numbers of flows with statistical QoS guarantees that can be admitted with efective envelope, we to determine maximum bound of end-to-end delay.

ACKNOWLEDGMENT

This research paper is partially supported by the Ministry of Higher Education Malaysia (MoHE). The authors would like to acknowledge the MoHE for their support in our research work.

REFERENCES

Beck F, Cholez T, Festor O, Chrisment I (2007). Monitoring the neighbor discovey protocol. Proc. Int. Conf. Comp. Global Inf. Tech., pp. 57-63.

Belhoul A, Sekercioglu YA, Mani N (2009). Mobility-aware RSVP: A framework for improving the performance of multimedia services over wireless IP-based mobile networks. J. Comp. Com., 32(4): 596-582.

Belhoul A, Sekercioglu YA, Mani N (2008). Mobility protocol and RSVP performance in Wireless IPv6 networks: shortcomings and solutions. Wireless Com. Mob. Comp., 8(7): 1183-1199.

Boorstyn R, Buchard A, Liebeherr J, Ottamakorn C (2000). Effective Envelopes: Statistical Bounds on Multiplexed Traffic in Packet networks. Proc. IEEE Int. Conf. Comp. Com., pp. 1223-1232.

Koodi R, Perkins CE (2007). Mobile Internetworking with IPv6. Wiley-Interscience, USA.

Le D, Fu X, Gu X, Hogrefe D (2007). E2T:End-to-End Tunneling Extension to Mobile IPv6. Proc. IEEE Consum. Com. Net. Conf., pp. 84-88.

Le D, Chang J (2010). Tunneling-based Route Optimization for Mobile IPv6. Proc. IEEE Int. Conf. Wireless Com. Net. Sec., pp. 509-513.

Lim HJ, Kim M, Lee JH, Chung TM (2009). Route Optimization in Nested NEMO: Classification, Evaluation, and Analysis from Memo Fringe stub prespective. IEEE Trans. Mobile Comp., 8(11): 1554-1572.

Liebeherr J, Patek S, Yilmaz E (2000). Tradeoffs in designing networks with end-to-end statistical QoS guarantees. Proc. IEEE Int. Workshop Qual. Serv., pp. 221-230.

Malekian R (2008). The study of Handover in Mobile IP Networks. Proc. IEEE Conf. Broadband Com. Inf. Tech. Biomed. Appl., pp. 181-185.

Malekian R, Abdullah AH, Saeed RA (2011). Cross-layer scheme for resource reservation based on multi-protocol label switching over mobile IP version6. Int. J. Phys. Sci., (In press).

Malekian R, Abdullah AH, Ding-Geng C (2011). ROMA: Determine the Maximum End-to-End Delay Based on a New Resource Reservation Method over Mobile IPv6 Routing Architecture. Australian J. Basic Appl. Sci., 5(4): 239-251.

Mellouk A (2008). End-to-End Quality of Service engineering in next generation heterogeneous networks. John Wiley and Sons Inc., USA.

Rabbat R, Laberteaux K, Modi N, Kenny J (2000), Traffic Engineering Algorithms using MPLS for service differentiation. Proc. IEEE Int. Conf. Com., pp. 791-795.

Vogt C, Bless R, Doll M, Kuuefner T (2005). Early Binding Update for mobile IPv6. Proc. IEEE Int. Conf. Wireless Com. Net., pp. 140-1445.

Yi ZZ, Xuefeng Z, Jia J (2009). Mobile IPv6 protocol research and development. Proc. Int. Forum Inf. Tech. Appl., pp. 313-317.