

PARALLEL AAA AND MOBILE IP REGISTRATION FOR HIGH PERFORMANCE
AND SCALABLE MOBILE ROAMING

by

Aykut Soner Demirkol

B.S, in PHYS., Bogazici University, 2005

Submitted to the Institute for Graduate Studies in
Science and Engineering in partial fulfillment of
the requirements for the degree of
Master of Science

Graduate Program in Computer Engineering
Bogazici University

2009

PARALLEL AAA AND MOBILE IP REGISTRATION FOR HIGH PERFORMANCE
AND SCALABLE MOBILE ROAMING

APPROVED BY:

Prof. M. Ufuk Çağlayan

(Thesis Supervisor)

Assist. Prof. Fatih Alagöz

Prof. Kemal Cılız

DATE OF APPROVAL: 29.01.2009

ACKNOWLEDGEMENTS

A thesis is extremely dependent to patience of the one that thinks, works on it and writes it. On the other hand, patience of a one in this fast forwarding world that everybody wants to have results instantaneously and judge instantaneously, comes all from their supporters. For me, there are too many supporters who gave a hand all the way to point where I am.

Firstly, I would like to express my gratitude to my thesis advisor who, each time, waited patiently for me to come with some worthy results and guide me how to construct a thesis. I shall thank to all my lecturers from primary school to graduate years who trained me through my life.

All of my friends never had a doubt about me and my work. They shared their knowledge, experience and with a sincere smile they patiently motivated me to go on. I will like to thank Alper Yegin. I found the subject of this thesis while I am discussing Mobile IP with him and he also gave me the initial background, support to work on it. My deep thanks to Berk Gulenler and old colleagues. He gave me hardware support through long simulation weeks and they helped me to spare some time for my thesis in my working hours. I am also grateful to Yunus Ot. He worked as my logistic department and catalyzed all the paper works for me.

My brother, Ilker Demirkol was the perfect reference to do what I do. He helped me in all aspects of life. My parents Muzeyyen Demirkol, Ilhan Demirkol and my sister Meltem Demirkol worked hard to bring out the potential which they always believe that lays in me.

Lastly, I am grateful to my lovely friend Derya Gulterler. Most of the time, I can not imagine how I could be able to struggle for something without her. She always supported me unconditionally and endlessly. She always helped me to decide on the path and motivated me till I reach the end of it. Thank you my fellow traveler.

ABSTRACT

PARALLEL AAA AND MOBILE IP REGISTRATION FOR HIGH PERFORMANCE AND SCALABLE MOBILE ROAMING

An important part of the communication technology currently depends on the wireless networking. With the increase in the connectivity needs, many types of wireless technologies have been deployed to ensure the coverage of the living areas using short and long range networks. Due to the access needs for efficient and continuous connectivity, interoperability became a very important issue. Mobile IPv4 is a well accepted protocol, standardized by IETF for such needs. Mobile IPv4 enables a wireless node to move from one infrastructure to another without disrupting the end-to-end TCP communication. Almost all IP based wireless technologies that are already developed or under development aim Mobile IP support.

Support for Authentication, Authorization and Accounting (AAA) architectures are also included in latter Mobile IP standards. IETF draft standard “RADIUS Mobile IPv4 extensions” defines new attributes and methods to provide AAA support for Mobile IPv4. This standard defines new interactions before starting the Mobile IP registration between a mobile node and RADIUS servers. The preliminary RADIUS server interactions increase the overall time needed for Mobile IP with RADIUS registration significantly.

In this thesis work, a new solution, named “Parallel AAA and Mobile IP Registration” is proposed to decrease the communication overhead associated with preliminary RADIUS server interactions. In the proposed solution, the existence of pre-established Foreign Agent - Home Agent security associations are assumed. A simulation model of the proposed solution and the RADIUS Mobile IPv4 extension standard is developed to compare their overall registration time performance. The simulation model also provides a scalability analysis of overall registration time. It is also shown that the proposed solution performs better under various communications link and server hardware settings.

ÖZET

YÜKSEK PERFORMANS VE ÖLÇEKLENEBİLİR MOBİL DOLAŞIM İÇİN PARALEL AAA VE MOBİL İP KAYIDI

Günümüzde kablosuz bağlantı teknolojileri iletişimde önemli bir yere sahiptir. Kullanıcıların daha hızlı, daha yaygın ve kesintisiz bağlantı talepleri, bu alandaki çalışmaların hızla artmasını ve ilerlemesini sağladı. Sonuç olarak, kullanıcılara hizmet vermek üzere kurulan ve kullanılan bir çok farklı altyapı ortaya çıkmıştır. Bu farklı altyapıları kullanırken, ortak desteklenen bir sistem ile kullanıcının altyapı türünden bağımsız olarak sürekli bağlı kalmasını sağlayacak bir teknoloji ihtiyacı doğmuştur. Bu sorunlara kalıcı çözüm bulmak için bir çok model geliştirildi ve hala geliştirilmektedir. Mobil IP bu modeller içinde sıyrılan ve IETF tarafından standartlaştırılıp kullanıma açılan, sektörde ve akademide kabul görmüş bir protokoldür. Mobil IP, kullanıcının aktif TCP bağlantılarını baştan kurmasına gerek bırakmayacak şekilde IP tabanlı her hangi iki ağ arasında, altyapıdan bağımsız bir şekilde dolaşmasına olanak sağlar.

Son kullanıcı ve servis sağlayıcı açısından kullanılabilirliğini ve esnekliğini arttırmak için Mobil IP ile AAA iletişimi entegre edilmiştir. AAA protokolünün desteğiyle kimlik denetimi, ilgili anahtarların dağıtımı ve muhasebe için data toplanması mümkün olmaktadır. Fakat AAA entegre edilmiş Mobil IP'de yeni bir oturum açmak için gereken zaman, Mobil IP kaydı öncesinde AAA mesajlaşmaları gerçekleşmesi gerekli kılındığından önemli ölçüde artmıştır.

Biz bu çalışmada ilgili AAA ve Mobil IPv4 iletişimlerini paralel gerçekleştirerek yeni bir çözüm önermekteyiz. Bu önerimizde AAA ve Mobil IPv4 standartlarını bozmadan, yeni bir oturum açmak için gereken zamanı kısaltmaktayız. Bu tezde önerdiğimiz çözümün analitik olarak incelemesi sunulduktan sonra servis sağlayıcıların kullanacağı alt ve üst yapıya uygun parametrelerle yaptığımız simülasyon çalışmalarının sonuçları gösterilmektedir. Önerdiğimiz çözüm, kayıt zamanı olarak daha iyi performans sergilemekte ve ölçeklenebilirlik açısından şu an kullanılan standard'a göre yakın ve daha iyi şartlar sunmaktadır.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS.....	iii
ABSTRACT.....	iv
ÖZET.....	v
LIST OF FIGURES.....	viii
LIST OF TABLES	xi
LIST OF SYMBOLS/ABBREVIATIONS.....	xii
2. OVERVIEW OF MOBILE IP WITH AAA	5
2.1. Overview of Mobile IP	5
2.2. Overview of Mobile IP with RADIUS	7
2.3. Related Work.....	9
2.3.1. Using Hierarchical Systems.....	9
2.3.2. Using Cryptographic Systems.....	11
3. OUR PROPOSED SOLUTION: PARALLEL MOBILE IP AND AAA	
REGISTRATION	13
3.1. Proposed Structure.....	14
3.2. Compatibility of Proposed Structure	15
3.2.1. Foreign Agent – Home Agent Mobile Security Association.....	15
3.2.2. When Parallel Communications Broke	16
3.3. Possible Security Drawbacks of Proposed Solution.....	17
4. ANALYTICAL PERFORMANCE ANALYSIS OF PROPOSED SOLUTION.....	18
4.1. Analytical Model for Mobil IP and AAA Communications	19
4.2. Analytical Performance Evaluation of Both Approach	20
5. PERFORMANCE ANALYSIS OF PROPOSED SOLUTION WITH SIMULATION	
MODEL	23
5.1. Simulation Model of Mobile IPv4 with Radius	23
5.1.1. Defining a Simulation Network Model from a Possible Service Provider	
Network	24
5.1.2. Referenced Computational Costs.....	26
5.1.3. Creating a Job Definition from each Steps of Mobil IP and AAA	
Communications	28
5.1.4. Calculating the Base Processing Time for Mobile IP Jobs	32

5.1.5. Event Sequence of Current Approach in Mobile IP.....	33
5.1.6. Event Sequence of Simulation Model of Proposed Approach	35
5.2. Our Simulation Environment: OPNET	36
5.2.1. Network Scheme Created in OPNET.....	37
5.2.2. Setting Job Processing Time in OPNET	37
5.2.3. Automatic Scaling of Job Resource Consumption	38
5.3. List of Input Sets Simulated	40
5.3.1. Link Delays Simulated	40
5.3.2. Network Node Hardware Simulated	41
5.3.3. Network Node Background Utilizations Simulated.....	41
5.4. Simulation Results	42
5.4.1. Overall Registration Time Results of Both Approaches	43
5.4.1.1. Effect of Link Delays.....	43
5.4.1.2. Effect of Hardware choice.....	52
5.4.1.3. Effect of Network Node Background Utilization.....	55
5.4.2. Scalability Results of Both Approaches	55
5.4.2.1. Effect of Link Delays	55
5.4.2.2. Effect of Hardware choice.....	55
5.4.2.3. Effect of Network Node Background Utilization.....	57
5.4.2.4. Background Utilization versus Dedicated Computational Power.....	61
5.5. Discussion of Simulation Results	66
5.5.1. Active Number of Mobile Nodes.....	67
5.5.2. Effect of Link Delays	69
5.5.3. Deciding Server Dedication for New Mobile IP Deployments	71
6. CONCLUSIONS	73
REFERENCES.....	76

LIST OF FIGURES

Figure 2.1. Mobile IP messaging between a Host and a MN	6
Figure 2.2. Mobile IP registration steps	7
Figure 2.3. Mobile IP with RADIUS authentication and registration steps	8
Figure 2.4. Normal communication path and new communication path.	10
Figure 3.1. Parallel authentication and registration steps of proposed solution	14
Figure 4.1. Network graph of the analytical model.....	19
Figure 4.2. Network graph and communication costs.....	20
Figure 4.3. Overall registration time versus unit time.....	21
Figure 4.4. Gain of proposed approach.	22
Figure 5.1. An example Service provider network.	25
Figure 5.2. Simplified picture of the service provider network.....	26
Figure 5.3. Presentation of the simulation network.	27
Figure 5.4. Messages of the original Mobile IP and Radius communication.....	28
Figure 5.5. OPNET network structure.....	37
Figure 5.6. OPNET task configuration.....	38
Figure 5.7. Setting a process cost to server hardware in OPNET.....	39
Figure 5.8. Assigning a job to server hardware in OPNET.....	39
Figure 5.9. Registration speed of the current practice under 10 ms inner communication delay	43
Figure 5.10. Registration speed of the current practice under 30 ms inner communication delay	44
Figure 5.11. Registration speed of the current practice under 50 ms inner communication delay	44
Figure 5.12. Registration speed of the proposed solution under 10 ms inner communication delay	45
Figure 5.13. Registration speed of the proposed solution under 30 ms inner communication delay	46
Figure 5.14. Registration speed of the proposed solution under 50 ms inner communication delay	46

Figure 5.15. Registration speed of the current practice under 100 ms inter communication delay	47
Figure 5.16. Registration speed of the current practice under 300 ms inter communication delay	48
Figure 5.17. Registration speed of the current practice under 500 ms inter communication delay	48
Figure 5.18. Registration speed of the current practice under 700 ms inter communication delay	49
Figure 5.19. Registration speed of the proposed solution under 100 ms inter communication delay	50
Figure 5.20. Registration speed of the proposed solution under 300 ms inter communication delay	50
Figure 5.21. Registration speed of the proposed solution under 500 ms inter communication delay	51
Figure 5.22. Registration speed of the proposed solution under 700 ms inter communication delay	51
Figure 5.23. Performance of the current practice under various FA hardware.	52
Figure 5.24. Performance of the current practice under various AAA server hardware....	53
Figure 5.25. Performance of the proposed solution under various FA hardware.	54
Figure 5.26. Performance of the proposed solution under various AAA server hardware.	54
Figure 5.27. CPU utilizations of network nodes in the current practice.	56
Figure 5.28. CPU utilizations of network nodes in the proposed solution.	57
Figure 5.29. Effect of FA background utilization to performance of the current practice	57
Figure 5.30. Effect of FA background utilization to performances of the proposed solution.	58
Figure 5.31. Effect of AAA server background utilization to performances of the current practice.	59
Figure 5.32. Effect of AAA server background utilization to performances of the proposed solution.	60
Figure 5.33. Performance of AAA servers under 75% background utilization. Overlaid performance graph.	61
Figure 5.34. Calibration of current practice to overlay result graphs.	62

Figure 5.35. Calibration of current practice to overlay to overlay result graphs. Closer look to saturation point.....	63
Figure 5.36. Effect of FA background utilization compared with slower hardware choice.	63
Figure 5.37. Effect of 50% AAA server background utilization to performances of the current practice, compared with slower AAA hardware choice.....	64
Figure 5.38. Effect of 50% AAA server background utilization to performances of the our solution, compared with slower AAA hardware choice	64
Figure 5.39. Effect of 75% AAA server background utilization to performances of the current practice, compared with slower AAA hardware choice.....	65
Figure 5.40. Effect of 75% AAA server background utilization to performances of the proposed solution, compared with slower AAA hardware choice	66
Figure 5.41. Rate of incoming request versus time.....	68
Figure 5.42. Performance comparison of the current practice and the proposed solution for very low link delays.....	71

LIST OF TABLES

Table 4.1. Classification of each communication pair in the Analytical Model.....	17
Table 5.1. Benchmark results of main hash functions.....	27
Table 5.2. Summary of Mobile IP job processing times.....	33
Table 5.3. Cell Residence Time.....	68

LIST OF SYMBOLS/ABBREVIATIONS

AAA	Authentication, authorization and accounting
AReq	Access request message
ARep	Access response message
ATM	Asynchronous transfer mode
CA-PKI	Certificate-based key infrastructure
CAs	Certificate authorities
CDMA	Code division multiple access
CoA	Care-of address
CPU	Central processing unit
DSL	Digital subscriber line
FA	Foreign agent
FAAA	Foreign authentication, authorization and accounting
GSM	Global System for Mobile communications
HAAA	Home authentication, authorization and accounting
HA	Home agent
HoA	Home IP Address
IETF	Internet engineering task force
IP	Internet protocol
ISP	Internet service provider
RFC	Request for Comment
RRP	Registration reply
RRQ	Registration request
MD5	Message-digest algorithm 5
MIP	Mobile IP
MN	Mobile node
MU	Mobile user
MSA	Mobile security association
NAT	Network address translation
NAS	Network access server
SHA1	Secure hash algorithm 1

SPI	Security parameters index
TCP	Transmission control protocol
UMTS	Universal mobile telecommunications system
USIM	Universal subscriber identity module
VOIP	Voice over IP
3G	Third generation mobile networks

1. INTRODUCTION

Communication and freedom are among the basic instincts and primary needs of the humankind. These basic needs gave rise to continuous rapid advancements in the technologies related to the communication area. Just fifty years ago Public Switched Telephone Networks (PSTN) started to be implemented around the world. It provided necessary infrastructure for the basic need of communication. But it did not brought much convenience in communication. When thirty years past over the initial PSTN deployments, first GSM specifications were published. With the developments in wireless technologies, more freedom in communication has been achieved. We became able to communicate when we are mobile and became more accessible. Today, we see that our needs have changed. Consumers want to be connected to the rest of the world at any time, with high capacity of transmissions, without interruption and at the most reasonable price possible. After many years of rapid developments and deployments in this field, we now reached to a very diverse communication infrastructures and technologies that are all simultaneously in use. Moreover, there are still numerous ongoing developments in communication technology that is going to bring faster, better exchange of information but also different standards and structures. This diversity has brought about the need for the connectivity of these various infrastructures. That is why, the interoperability and roaming constitutes two of the hot networking topics of our age.

We expect to continue to have the co-existence of different communication technologies. We will basically have wired and wireless communication technologies and there will be many fractions in these technologies. In recent years most of the new technologies have been developed with the idea of co-existence with current solutions. This natural behavior of evolution improves the deployment speed of developments. It brings the freedom to use a new solution without completely abandoning the old one.

Choosing the cheapest or the best fitting product for our needs is a gift of diversity. But this mixture of technology has also negative side effects. In order to reach a certain level of uninterrupted connectivity we must have the capacity to interoperate through various infrastructures. Transitions in these roaming processes must occur in real time and

with insignificant delay. In order to deal with this interoperability and roaming requirements, some solutions have already been designed and developed. As one of the solutions, Mobile IP is a well known and accepted protocol which is supported by many infrastructures, standards and products that are currently in the development process or are already in use. Today, most of the deployed technologies like WIMAX, 3G and most of IP networks support Mobile IP. It is an open standard defined by the Internet Engineering Task Force (IETF) that allows a mobile user (MU) to keep the same IP address, stay connected, and maintain the ongoing applications while roaming between different IP network domains [1].

The main idea of Mobile IP is to enable a mobile node to move freely from one connection point to the Internet to another without disrupting the TCP end-to-end connectivity [2]. It provides an efficient mechanism for mobility support within the Internet [3]. One of its strengths is the backward compatibility. The fundamental assumption behind the development of Mobile IP was backward compatibility with the existing Internet infrastructure based on TCP/IP protocol suite which was originally developed for fixed networks [4].

In order to make it more practical and integrable to current operator environments, support for authentication, authorization and accounting (AAA) protocols such as RADIUS were added to Mobile IP standards [6]. However, using Mobile IP with AAA protocols also has some critical disadvantages. With the addition of new preliminary AAA authentication messaging, the overall registration time of Mobile IP increased significantly.

In this thesis, we provide a solution, namely “Parallel AAA and Mobile IP Registration”, to decrease the communication overhead caused by RADIUS integration to Mobile IP. In our proposal we used the fact that the RFC 2977 [7] stated: the primary reason for the communication cost in Mobile IP is the time required for communications of widely separated nodes. It is also stated in several studies that inter-domain communications, which are the long distance communications, are the main reasons for delay in overall Mobile IP registration [8]. Our solution significantly decreases the inter-domain communication delays by defining a parallel AAA and Mobile IP communication scheme.

We identify requirements of sequential Mobile IP with AAA and show that these requirements can be fulfilled by other methods and/or business models. We present the proposed structure and state how exceptional cases can be handled. An analytical model is presented to compare theoretical performance evaluation of current approach and proposed solution. We define a simulation model and run numerous simulations on various link, hardware scenarios. We analyze the simulation results in terms of registration speed, scalability pattern and show that our proposed solution is outperforming current practice. Moreover, we discovered that server dedication is not best Mobile IP deployment choice. Instead, current AAA structures can be used to gain better performance. In our opinion, this finding can provide valuable contribution to business decisions at new Mobile IP deployments.

The remaining part of this thesis is organized as follows:

Chapter 2 describes the Mobile IP protocol and RADIUS support for it. Brief details of both protocols are presented in this chapter. In addition, currently available solutions for the registration delay problem are categorized and explained.

In Chapter 3, we describe our proposed solution “Parallel Mobile IP with RADIUS”. Our proposed messaging sequence of Mobile IP with AAA is also explained. Certain assumptions that we made is stated and the feasibility of these assumptions is discussed.

In Chapter 4, an analytical model is defined for the proposed solution. We investigate the performance results of proposal and current approach analytically. The comparison and discussion of the performance results are also presented.

In Chapter 5, simulation analysis for Mobile IP with AAA is presented. We provide the simulation model and simulation environment for our proposal and current approach. We explain various link and hardware settings that are used in the simulations and conclude the chapter with presenting simulation results and their discussions.

Chapter 6 concludes this thesis by summarizing our findings and presenting further potential improvements of this work.

2. OVERVIEW OF MOBILE IP WITH AAA

As we explained in Introduction section, Mobile IP is a standardized Internet Engineering Task Force (IETF) protocol [3]. Its main objective is to provide mobility and keeping end-to-end TCP connectivity while clients are roaming between different networks and/or infrastructures. In this section we firstly introduce Mobile IP in detail and then present Mobile IP with RADIUS. In the last subsection we will give related works on the subject.

2.1. Overview of Mobile IP

Mobile IP mainly consists of registration and tunneling processes. Each mobile user has a public global IP called Home IP Address (HoA). All messages sent to the mobile user are destined to his HoA. But HoA is actually handled by an interim node called Home Agent (HA). HA is responsible for keeping users current locations which are called Care-of Address (CoA). When a mobile user connects to a new network, it is responsible to update CoA through Mobile IP registration processes. That is how users store their up-to-date location information in HA. When a packet arrives that is sent to HoA, HA tunnels the packet to the Care-of Address of corresponding user. At the other side of this tunnel, another node called Foreign Agent (FA) or mobile user (Mobile Node) itself reside. When users are assigned a new private IP address by the networks they are connected, this information must be kept in some interim node. FA is responsible for keeping this CoA – private IP relation. It handles packets destined to CoA, de-tunnels and delivers original packets to corresponding mobile user. If FA does not exist, for example in case where Mobile Node can have a public global IP by a DHCP server, then Mobile Node (MN) must carry the role of de-tunneling by itself. In that case CoA must be a public IP that is accessible directly by HA.

Figure 2.1 illustrates a host messaging with a MN. Mobile IP messaging between users consists of following steps: A host sends a message to HoA of MN. HA tunnels this message to CoA of MN. FA de-tunnels and sends the packets to MN Private IP. After receiving the packets, MN sends its response to FA, which behaves as gateway for MN.

FA can tunnel response to HA or send it to the host directly. This choice is a matter of performance-security trade-off, but we will not go into detail of this in our work.

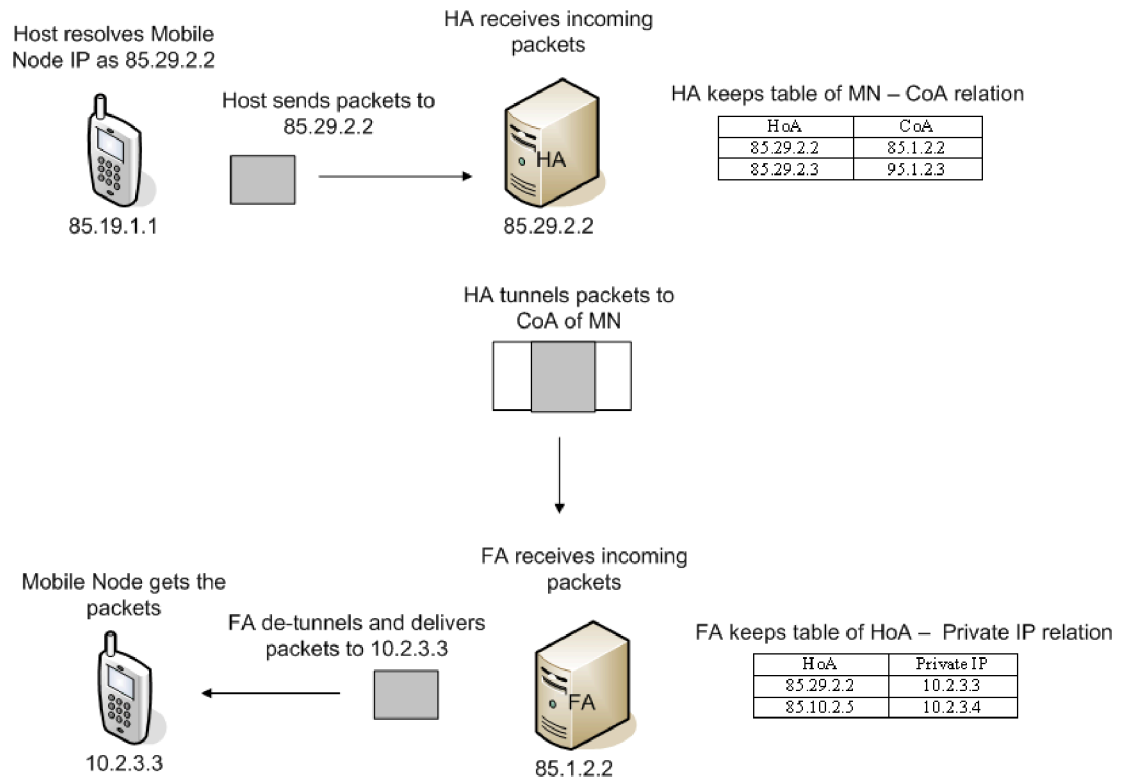


Figure 2.1. Mobile IP messaging between a Host and a MN

Since a mobile user must inform HA about its current location (CoA), when MN goes into a new network and takes a new CoA, it has to initiate a registration process for sending its new CoA to HA. Figure 2.2 illustrates the Mobile IP registration process for a MN. Registration process consists of the following steps: Upon receiving FA advertisement, MN joins to network and creates a Registration Request. FA processes the request, put the MN to pending list and relay the request to HA. HA authenticates the request with the Mobile Security Association (MSA). If HA authentication is successful, HA changes the recorded CoA, creates a Registration Reply and sends it to FA. FA processes the reply, if result is success, puts the MN in active user list and relays the response to MN.

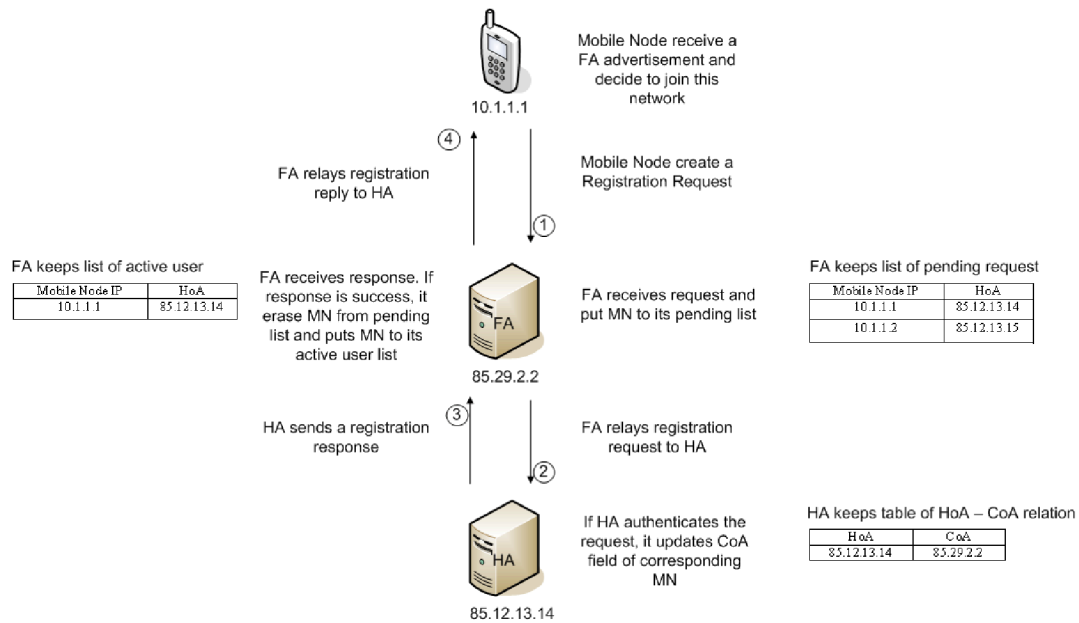


Figure 2.2. Mobile IP registration steps

2.2. Overview of Mobile IP with RADIUS

The basic Mobile IP standard [3] lacks crucial properties such as key distribution and support of accounting structures. On the other hand, authentication, authorization and accounting (AAA) systems are well accepted and widely deployed solutions that provide these properties. An integration standard released in 2000 [7] to define Mobile IP requirements of AAA. By using that integration standard, extensions [6, 9] developed for AAA protocols RADIUS and DIAMETER. The extension standards do not imply basic changes on AAA protocols rather the use of these protocols with Mobile IP is defined.

To combine Mobile IP with RADIUS, an AAA authentication step has been defined before the Mobile IP registration step [6]. Foreign Agent first checks if the user can be authenticated, then communicates with Home Agent to register Mobile Node's Care-of Address. If no Mobile Secure Association (MSA) exists between HA and MN, then HA consults the Home AAA (HAAA) to have proper MN-HA key and nonces for creating Mobile Node – Home agent (MN-HA) MSA.

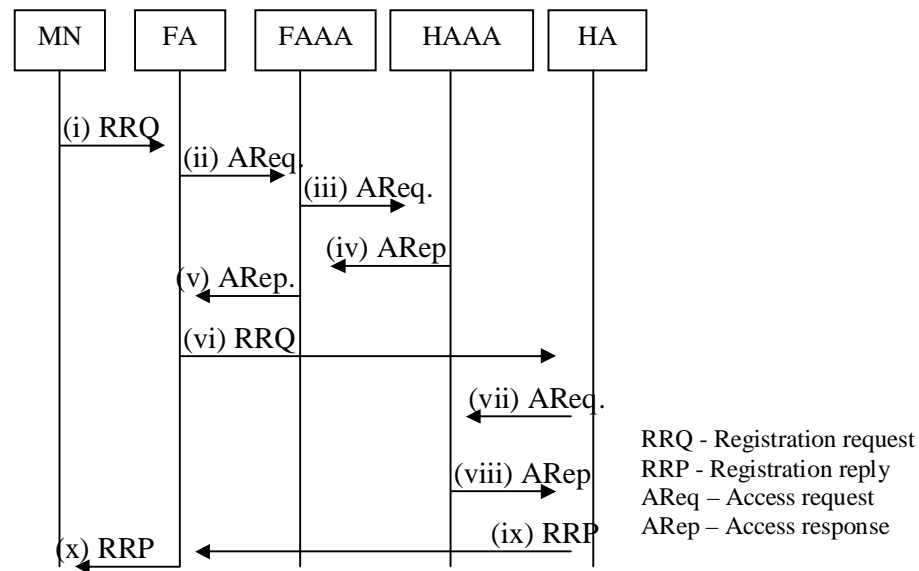


Figure 2.3. Mobile IP with RADIUS authentication and registration steps

Figure 2.3 illustrates Mobile IP with RADIUS registration which consists of the following steps:

- i) MN sends Registration Request (RRQ) to FA.
- ii) FA creates a RADIUS Access Request message (AReq) to its AAA server (FAAA) with the data it took from RRQ.
- iii) If FAAA does not have information about the MN it forwards request to HAAA.
- iv) HAAA authenticates MN. It creates RADIUS Access Accept/Deny message (ARep) and sends it back to FAAA.
- v) FAAA forwards the ARep to FA.
- vi) If HAAA/FAAA sends accept message to FA and confirms that MN is authenticated, FA relays the RRQ created by MN.
- vii) After receiving RRQ, HA sends AReq to HAAA to authenticate MN and take necessary key and challenges to create MSA.
- viii) HAAA sends corresponding Access Response to HA.
- ix) HA authenticates the registration request of MN, creates and sends Registration Reply (RRP) message to FA.
- x) FA processes RRP and forwards it to MN.

2.3. Related Work

Although fast registration is an essential property, overall registration time is increased significantly with the integration of RADIUS to Mobile IP. This drawback, i.e., the delay in registration time has been a hot research topic. There have been numerous studies and proposed solutions for this problem. Most of the studies attacked to the main reason of the delay; the inter domain communication time. As the initial specification of AAA integration standard [7] foresaw and the theories and simulations proved [8], communication delay between foreign network and home network creates the main part of overall registration delay. Because the Mobile Security Association resides between Mobile Node and Home AAA, the registration communication will be between foreign and home domain. Solutions to this problem are centered on either completely removing the necessity on the inter-domain communication or decreasing the number of steps in the communication by new cryptographic operations [19, 20] and/or trust relations [12] and/or hierarchical AAA positioning [10, 11]. Furthermore, some of the solutions are effective at first authentication attempt, while others provide the best solution at second and later authentication attempts. We can mainly categorize all these diverse approaches according to their addition to the current Mobile IP with AAA structure. Namely, we can categorize the solutions as the one that use hierarchical systems and that use cryptographic systems.

2.3.1. Using Hierarchical Systems

One of the basic approaches to decrease the registration delay is to create hierarchical AAA servers. Creating a Broker infrastructure by using USIM protocol is a way to achieve this goal [10]. In this solution a Broker is thought as an interim AAA server with some features added. When a Foreign AAA server wants to authenticate a client, it sends its request to a Broker AAA. Broker AAA communicates with Home AAA and attains some challenge-response pairs for further requests. At the next login attempt, Broker AAA uses these challenge-response pairs to authenticate the client. By geographical and hierarchical distribution of Broker AAAs, shorter authentication paths can be achieved. Hence, the rate of MN requests that requires inquiry of geographically distant, Home AAAs will be decreased.

A similar approach depends on creating securely associated, hierarchically adjacent Foreign AAA servers [11]. As with the broker-based infrastructure this solution also speeds up the second authentication process of the MN registration. When a user is already authenticated through a Foreign AAA server, if a new Foreign AAA server is used at next login attempt, the new Foreign AAA communicates with the former instead of communicating with Home AAA server as shown in Figure 2.4. This solution provides a similar AAA formation as the broker infrastructure do as described above. By geographically shortening authentication path, this solution speeds up the overall registration process.

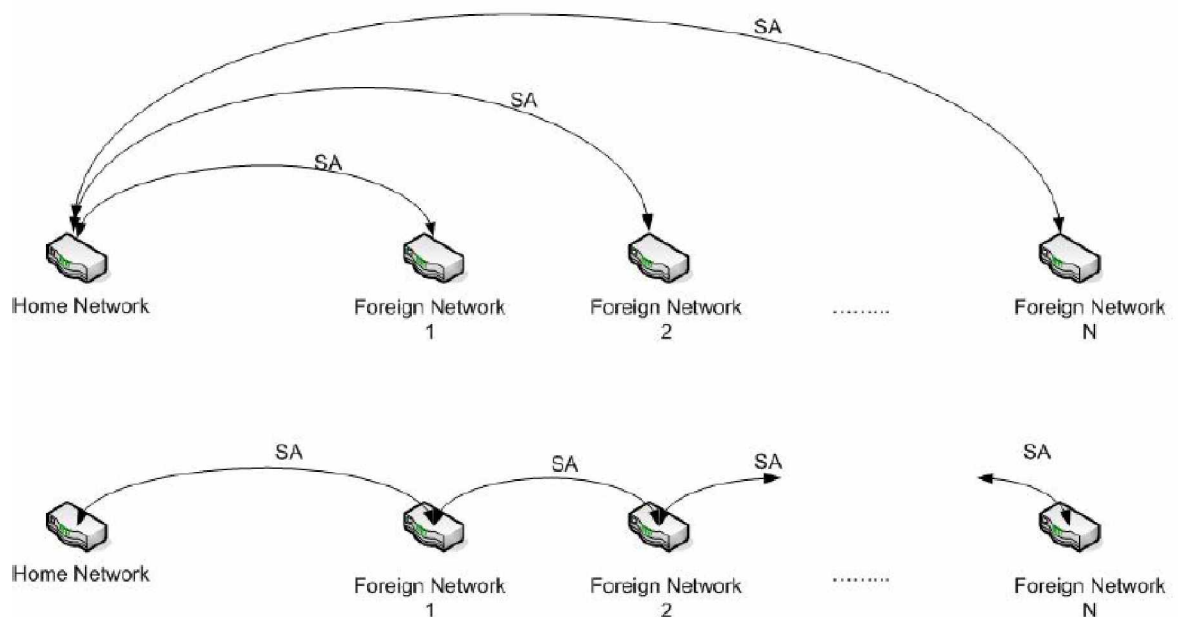


Figure 2.4. Normal communication path and new communication path.

Donghai et al. defines a hierarchical Mobile IP structure that uses Foreign Agent network with necessary security associations between FAs [12]. With the help of the specialized Foreign AAA server, Foreign Agent is able to create a trust relation among each other. When a client connects to any FA, the new FA find out the former FA and request the formers one to tunnel the incoming packets. With this approach, fast mobile movements are expected to cause less packet loss.

2.3.2. Using Cryptographic Systems

Researches on AAA cryptology in Mobile IP basically investigate better key or nonce exchange mechanism to achieve scalable, secure structures and less inter-domain communication. Some of the works on this subject focus on increasing integrity, anonymity of communications while decreasing cost of key exchange mechanisms. On the other hand, few researches investigate new cryptographic deployments for decreasing inter-domain communications.

To increase scalability of key exchange mechanism and to improve security features Certificate-based Key Infrastructure (CA-PKI) [13, 14, 15, 16] solutions had been proposed. Idea of using CA-PKI is creating scalable networks in terms of key derivation and distribution. As initial IETF draft [13] stated if pair of keys used for each pair of nodes, node keys required will be $N(N-1)/2$ for N nodes. For a large network, creating and distributing these keys will not be feasible. Instead of on demand key distribution approach, with the help of trusted third parties like Certificate Authorities (CAs), necessary security associations can be created by using CA-PKI.

With similar concepts, Identity-based key mechanisms [17, 18, 19] had been proposed by some researches. Identity-based mechanisms aim to reduce the intensive computation requirement of CA-PKI. It also helps creating anonymity in public key structure by separating user identity and public key [18].

Although these mentioned cryptographic infrastructures improve the security, in mean time increase cost of computation, most of them had little intention on speeding up registration process of Mobile IP. There are other researches that are focusing to this issue. One of the common approaches of these studies is making Foreign AAA end point of authentication as long as it can be. Creating long life time keys by re-using session keys [20] and applying a new key cryptology that enables inter-domain authentication are examples of this approach. Both researches provide faster second or latter authentication process. Creating long life time keys lets Foreign AAA to authenticate same user multiple times without communicating with Home AAA for a long time. One of the main drawbacks of this concept is security concerns. It is foreseeable that a key that do not

expire for a long time period can create a security hole in whole system. On the other hand, in [20] after the first registration, the Foreign AAA proposed to replace Home AAA. In their proposed commitment scheme, Foreign AAA cannot reveal key information. Moreover, by keeping some pairs of keys, FAAA is still able to produce necessary information to authenticate user.

3. OUR PROPOSED SOLUTION: PARALLEL MOBILE IP AND AAA REGISTRATION

As we noted before, the initial specification of AAA integration standard foresaw that communication delay between foreign network and home network constitutes the main part of overall registration period [7]. Moreover, simulation studies on the Mobile IP with AAA registration performance prove this idea [8]. In the previous section, we summarized some of the research studies on the subject. Most of the solutions target a faster authentication mechanism for the second and latter registrations by introducing new trust relations or cryptographic operations. On the other hand, in this thesis we provide a solution that also speeds up first registration attempt as well as latter attempts.

In our proposal we try to overlap inter-domain communications and run AAA and Mobile IP registration simultaneously. Overlapping these two long periods of communications can dramatically speed up overall registration process. We worked on the IETF draft that defines RADIUS extension for Mobile IP [6] and investigated the requisites of sequential communications and try to find out if these requisites can be fulfilled in other ways. We figured out that parallel processing does not break AAA and Mobile IP structure individually. The original standard [6] does not bind these two protocols. In fact it requires Mobile IP and AAA protocols to run independently one after another. Moreover, AAA registration process does not submit any user data to FA to start a registration process. FA is able to run independent of AAA communication but in this case HA may not trust FA. The only operational dependency between AAA and Mobile IP registration is creating FA-HA Mobile Security Association which requires AAA to run before Mobile IP. Authentication and registration both occur with pre-established HA-HAAA, MN-HAAA Mobile Security Associations and a dynamically created FA-HA Mobile Security Association. If we can justify that there can be also be a pre-established security association between FA and HA, then it is theoretically acceptable to run Mobile IP registration and AAA authentication in parallel.

3.1. Proposed Structure

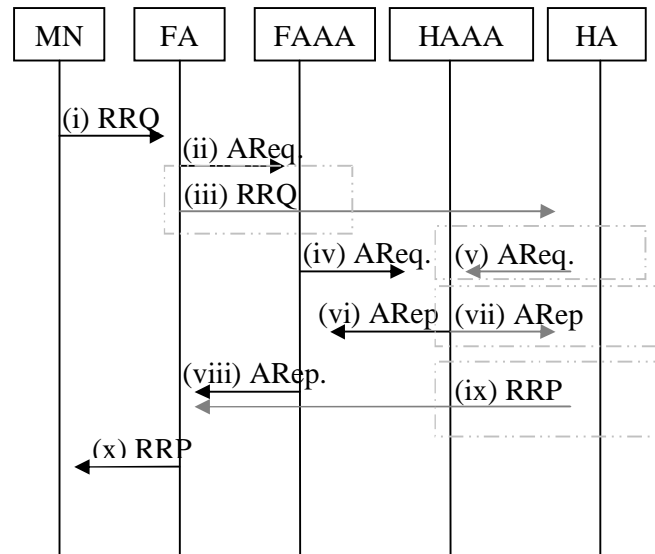


Figure 3.1. Parallel authentication and registration steps of proposed solution

Our proposed solution does not imply fewer communications steps. There are still 10 steps of communication as it is defined in draft standard [6] but in our solution some of the steps occur simultaneously enabling time saving. Moreover, no change is required in the packet contents in our solution, and hence, the same packet structure is used which is defined in the draft standard. As illustrated in Figure 3.1, the proposed simultaneity starts at step (2) where FA does not wait Access Reply before starting Mobile IP Registration. The sequence of the proposed solution is as follows:

- i) MN sends Registration Request (RRQ) to FA.
- ii) FA creates an RADIUS Access Request message (AReq) based on the information from RRQ and sends it to AAA server (FAAA).
- iii) At the same time with step (2-a), FA relays RRQ to HA.
- iv) If FAAA does not have information about the MN, it forwards the request to HAAA.
- v) At the same time with step (3-a), HA sends AReq to HAAA to have the necessary key and challenges for creating MSA.

vi) HAAA authenticates MN, creates RADIUS Access Accept/Deny message (ARep) and sends it back to FAAA.

vii) At the same time with step (4-a), HAAA sends the corresponding Access Response to HA.

viii) FAAA forwards the ARep to FA.

ix) At the same time with step (5-a), HA creates Registration Reply (RRP) message and sends it to FA.

x) FA relays Registration Reply (RRP) message and sends it to MN.

3.2. Compatibility of Proposed Structure

The proposed solution does not enforce any major changes that would conflict with the current standard. The major operational change among network nodes will be at Foreign Agent. Home AAA, Foreign AAA, Home Agent, Mobile Node will behave as usual. But there are some cases where the proposed system may cause a different resultant CoA to be kept in Home Agent when parallel communication breaks. In this subchapter, our justifications for assumptions, cases where the proposed solution results different CoA to be kept in HA and possible drawbacks of the proposal is covered.

3.2.1. Foreign Agent – Home Agent Mobile Security Association

The main assumption of the proposed solution is establishment of Foreign Agent – Home Agent security association prior to the registration process. This assumption has no compatibility conflict with the current practice of Mobile IP since the base standard [6] does not force FA to request a FA-HA MSA to be created. When FA creates a request to FAAA it may or may not ask an association to be created by setting appropriate flags.

On the other hand, practicality of key exchanges to create this MSA must be discussed. In daily usage of Mobile IP, we expect operators to not let any unknown FA to access their infrastructure. Current network security solutions will cause requests from unauthorized FA to be silently discarded. We do not expect operators to let an unknown FA to send IP packets to HA that will possibly reside in operator data warehouse. This idea drive us to believe that before an operator give service to a foreign network, owner of this

foreign network will have to get in touch with the operators. Probably after some contract been signed, operators will let FAs to give Mobile IP service. We believe that key exchanges can be done through this initial offline communication. A FA-HA MSA can be generated by assigning some key pairs to FA and HA and giving the necessary key to FA owner.

Moreover, plenty methods or business models can be designed to achieve this trust relation. For example, zero-touch FAs that are distributed by the operators which contain pre-entered keys can be a solution for this offline MSA creation. Developing software solutions for FAs to periodically maintain key exchange with the operator can be another approach. More solutions can be devised that enables the mentioned trust relation.

3.2.2. When Parallel Communications Broke

Our system may need to have an additional step for the case that FA does not start the Mobile IP registration for some reason, although there is a successful AAA authentication. In illustration of current practice at Figure 2.3, this corresponds to not starting (6) although (5) result in success. This is not a drawback for roaming cases, since in either way the client will not be able to connect to the new network. In the current approach or the proposed one, roaming will not occur due to FA rejection. For such a case, in current practice the FA have chance to not start Mobile IP registration although there is a successful AAA authentication. In our proposal, FA will be sending registration request that will successfully register new CoA but will discard the reply or will not give service although reply is a success. There will be a difference in resultant states between the current practice and our approach. In our approach this special case ends with a change in CoA, however, CoA remains same in current practice.

Change in CoA does not create a practical problem, since client will not be able to use Mobile IP due to FA rejection in either way. In the next registration attempt, CoA will be showing new registered value and both approaches will be in same state of CoA. For any further concerns, FA must inform HA to revert the change made. We think that currently there is not a practical need for such an extra action. But if needed, we foresee that, this can be handled by some extra messaging and buffering.

3.3. Possible Security Drawbacks of Proposed Solution

For the cases where AAA rejects the request, FA will be already sent the messages to HA and start Mobile IP registration. This will not be a security leak because HA, before changing HoA, first authenticates MN through HAAA communication as shown in Figure 2.3 as Step 7 and 8. If FA has an authentication fail reply from FAAA servers, we expect HA to have same fail reply from HAAA servers. Therefore, FA will have Mobile IP Registration Deny from HA and Authentication Deny from FAAA at the same time. In this case, FA can simply forward the RRP to notify MN about result, while still not letting the node to access network due to AAA authentication deny.

Our base assumption is that there can be a pre-established Foreign Agent – Home Agent security association. This idea can have practical difficulties as we mentioned earlier. From the security perspective, by considering the currently accepted pre-existing associations like HAAA-MN or HAAA-HA, we do not think that assuming one more association to pre-exist will significantly weaken the security infrastructure.

In our proposal, the key step is the Foreign Agent's parallel Mobile IP and AAA registration request. For any reason if client's registration request fails, our solution will be wasting nearly two times more resource compared to the original structure because of the unnecessary Mobile IP messaging. This can cause flood attacks to be more effective. For the current practice there is only one communication path to be flooded FA-FAAA-HAAA with wrong authentication information. In our structure there will be two communication paths FA-FAAA-HAAA and FA-HA-HAAA-HA-FA. That means, there will be almost two times more communication capacity loss due to unnecessary messaging. We think that this security drawback is tolerable because messaging cost of Mobile IP with AAA is in ignorable amount when compared to the current link capacities deployed in the operator infrastructures.

4. ANALYTICAL PERFORMANCE ANALYSIS OF PROPOSED SOLUTION

We explained current practice and the proposed solution for Mobile IP with AAA in earlier chapters. In this chapter, an analytical model is defined for the proposed solution. We provide analytical performance results of the proposal and current approach. The comparison and discussion of the performance results are also presented.

Transmissions, which occur between two network nodes who reside in same network or adjacent networks, are called Inner-domain communications. Whereas inter-domain communications refer to transmissions that occur between two network nodes that does not reside in same or adjacent networks. Foreign Agents and Mobile Nodes are assumed to be in same networks. Therefore, messaging between them is categorized as inner domain communications. On the other hand, Home AAA server is placed in the operator data house which is probably multi-hop away from FA. Therefore, messaging between them is categorized as inter-domain communications. Full list of this classification can be found in Table 4.1.

Table 4.1. Classification of each communication pair in the Analytical Model

Inner Domain Communications	Mobile Node - Foreign Agent, Foreign Agent - Foreign AAA server, Home AAA server - Home Agent
Inter Domain Communications	Foreign Agent - Home Agent, Foreign AAA server - Home AAA server

To propose an analytical model, we assume that there is no saturation or scalability problem in the network nodes, such that, all nodes accepts and processes each request without any delay. Furthermore, we assume that each inner-domain communication has equal transmission time and each inter-domain communication has equal transmission time in the proposed analytical model. If we compare transmission speed of current backbone infrastructures to small packets of RADIUS and Mobile IP communications, we can

conclude that size of these small packets do not affect transmission speed. Therefore, we discard the difference in packet lengths of each messaging and assume that a fix packet length can be used in the proposed model.

4.1. Analytical Model for Mobil IP and AAA Communications

In our analytical model, a simple network that has one Mobile Node connected to a Foreign Agent that is connected to a Foreign AAA server and a Home Agent is used. Both Home Agent and Foreign AAA server is connected to a Home AAA server as illustrated in Figure 4.1.

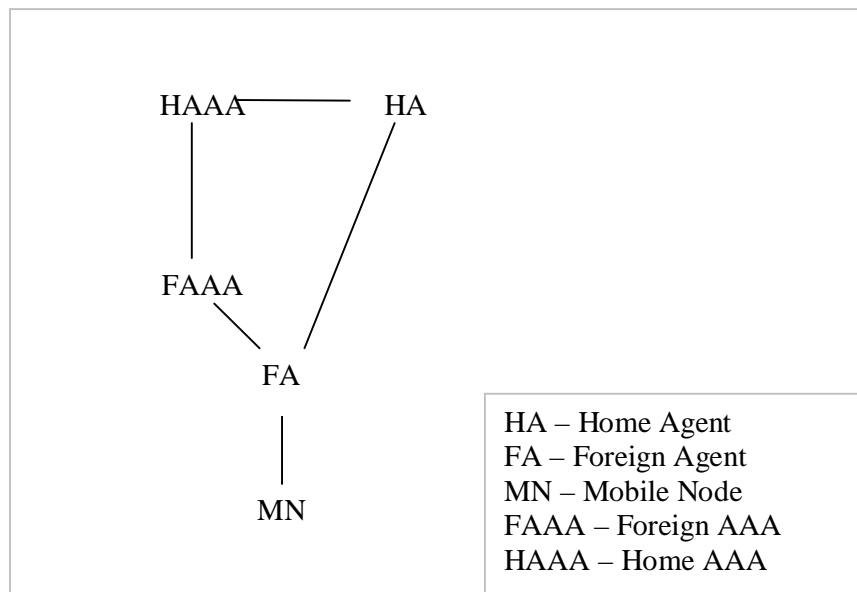


Figure 4.1. Network graph of the analytical model.

We assign X units of transmission time for all inner domain communications and Y unit of transmission time for all inter domain communications. Figure 4.2 illustrates resultant transmission times on the network graph.

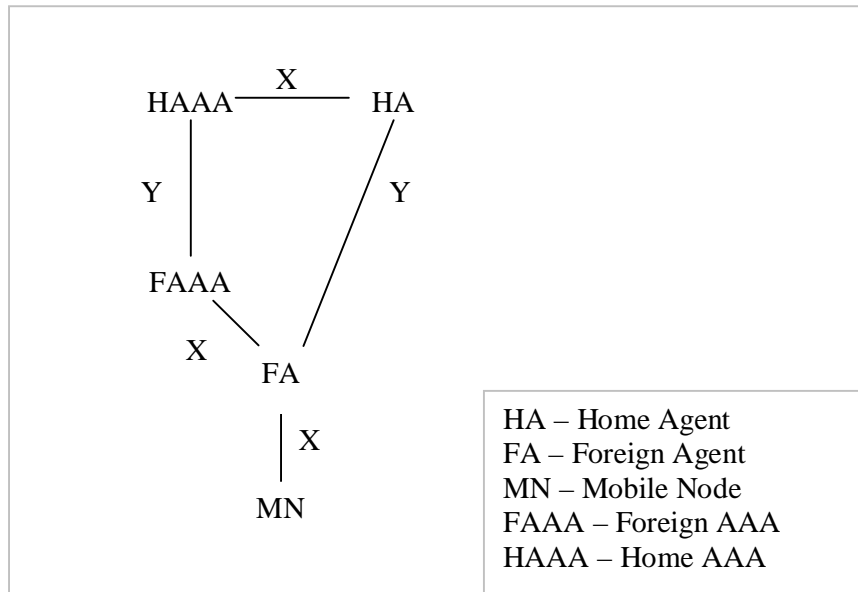


Figure 4.2. Network graph and communication costs.

4.2. Analytical Performance Evaluation of Both Approach

Current standard defines following communications to occur sequentially (Figure 2.3): MN-FA, FA-FAAA, FAAA-HAAA, HAAA-FAAA, FAAA-FA, FA-HA, HA-HAAA, HAAA-HA, HA-FA, FA-MN.

If our transmission assignments are applied, this sequential communication has an overall registration time of: $t_x + t_x + t_x + t_y + t_y + t_y + t_x + t_x + t_y + t_x = 6t_x + 4t_y$

Proposed system, on the other hand, has simultaneous communications except in steps (i) and (vi) illustrated in Figure 3.1. The communication splits in to two parallel messaging branches at step (i) and branches unifies at step (vi). FA-HA, HA-HAAA, HAAA-HA, HA-FA communications constitutes first branch. FA-FAAA, FAAA-HAAA, HAAA-FAAA, FAAA-FA communications constitutes second branch. If our transmission assignments are applied, it is found that both branches have $2t_x + 2t_y$ overall time. If we add MN-FA (i) and FA-MN (vi) steps, overall communication become $4t_x + 2t_y$.

Setting t_x and t_y to 1 unit time and increasing t_y will yield performance graph presented in Figure 4.3. As we can see when t_y value is 6 times larger than t_x , overall registration time is doubling in the current practice when compared to the proposed solution.

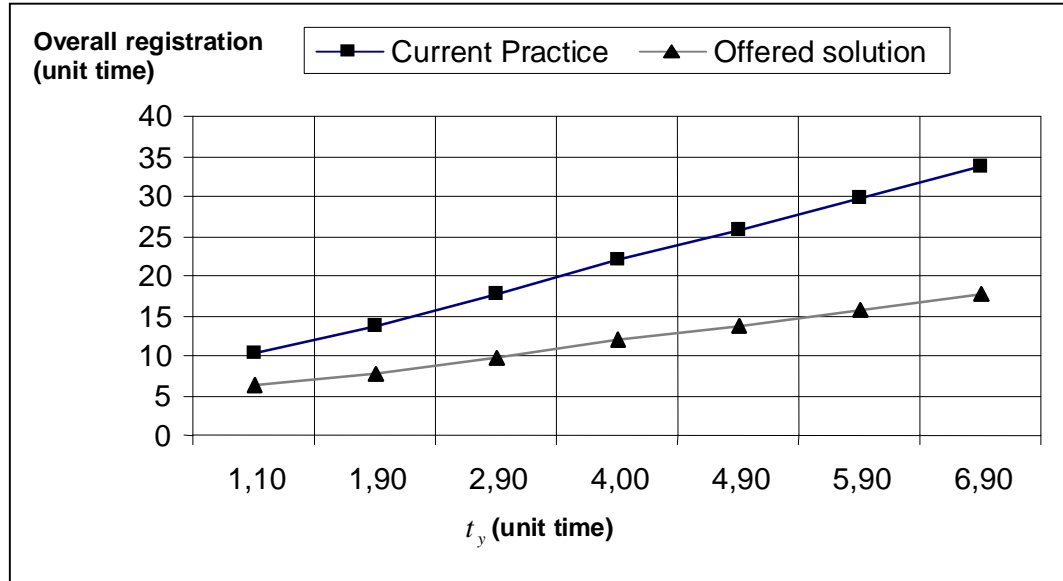


Figure 4.3. Overall registration time versus unit time.

Performance gain of the system can be defined as the current solution overall registration time divided by the proposed solution overall registration time. If our transmission assignments are applied, gain is found $6t_x + 4t_y / 4t_x + 2t_y$.

$$\text{Performance gain of the proposed solution} = 6t_x + 4t_y / 4t_x + 2t_y \quad (4.1)$$

If we assign t_x and t_y to 1 unit time and increase t_y while keeping t_x constant, gain graph, as illustrated in Figure 4.4, is found.

If inter-domain transmission time (t_y) increases, inner-domain transmission time (t_x) becomes more negligible. By simplifying negligible t_x , the Equation 4.1 becomes $4t_y / 2t_y = 2$. Figure 4.4 also proves this; with the increase in t_y , gain value tends to reach 2.

Therefore, best performance gain is occurred when inter-domain transmissions time is larger than inner-domain transmission. We expect this to be the general case due to definitions of domain communications as we explained earlier.

On the other hand, when all transmission times assumed to be equal, resultant gain will be $10/6=1,67$. Therefore, even the inner and inter communication times are at similar values, registration speed is improved 67%.

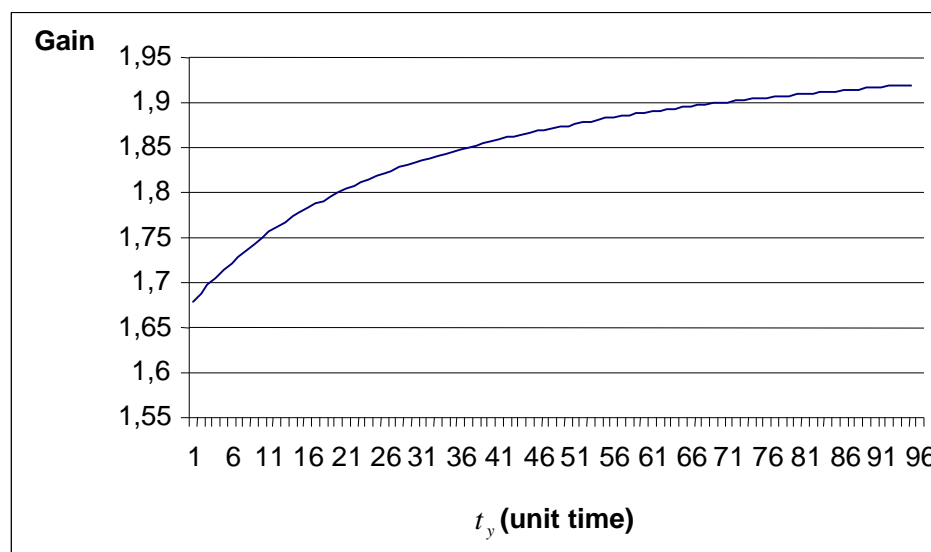


Figure 4.4. Gain of proposed approach.

By an analytical performance measure, we presented that the proposed solution is outperforming the current practice. Especially, when inter-domain communications are 6 times slower than inner-domain communications, the proposal provides 2 times faster registration speed.

5. PERFORMANCE ANALYSIS OF PROPOSED SOLUTION WITH SIMULATION MODEL

As stated in the beginning of Chapter 4, to provide an analytical model, we have to have certain assumptions, such that, no load exist on network nodes. Due to these assumptions and simplifications, an analytical model cannot provide a scalability analysis. However, in practice, capacity limits will cause delays, loads on the nodes can affect performance and saturations can occur. Therefore, scalability is one of the main concerns in real deployments.

In this chapter, for analyzing the proposed solution in terms of scalability and registration time, we provide a simulation analysis. The analysis presents more precise performance results in a more realistic, fluctuating environment. Firstly, the simulation model than simulation environment that we implement our model is described. This chapter is concluded by results of the analysis and discussion of the findings.

5.1. Simulation Model of Mobile IPv4 with Radius

Incoming Mobile Nodes are dynamic entities of the model. Rest of the network nodes are resource entities. Pre-assigned and constant link speeds, packet lengths and process time cost are used. Therefore, a discrete simulation model is provided.

In the model, each resource entity behaves as a First in First out (FIFO) queue. Further detail of the queuing system is handled by simulation tool. Each process (Mobile IP jobs) is defined in section 5.1.3. At same section, detail of the Mobile IP jobs is provided with the list of the cryptographic operations occurs in the processing of the jobs. In section 5.1.4, base processing cost of each Mobile IP job is found by multiplying cryptographic operations of them to the reference time values presented for the defined hardware architecture in section 5.1.2. Other operations on entities, such as a database search at AAA servers, are not considered in simulation study.

In the model, number of all network nodes except Mobile Node is predefined. In section 5.1.1, network graph and distribution of nodes over network is presented. Movements of Mobile Nodes are not directly subject of this thesis. Therefore, Mobile Nodes assumed to be stable. For further analysis on the result, in section 5.5.1, an empirical data that define a cell residential time is provided. The case where Mobile Node cannot be authenticated or Foreign AAA servers have cached information about Mobile Node is not considered in simulation study. It is assumed that MNs provide valid credentials and do not need to re-authenticate through same FAAA. Foreign AAA servers assumed to not have early information about Mobile Node, such that, a proactive behavior.

Primary events in the model; are start of a Registration Request (RRQ) made by a new Mobile Node and arrival of a Registration Reply (RRP). Sequence of secondary events depends on the Mobile IPv4 approach that is simulated. It varies between current approach and proposed solution as explained in subsections 5.1.5 and 5.1.6.

Network nodes; Foreign Agent, Home Agent, Home AAA server, Foreign AAA server is our resource entities. They are assumed to have infinite queue length to simplify the analysis of loads exercised by requests. Assumed job processing times for each node is provided in subsection 5.1.3.

Main performance measure is overall registration time for a Mobile Node which is defined as the time period between Registration Request and Registration Reply. Secondly, bottlenecks points and scalability patterns are presented.

5.1.1. Defining a Simulation Network Model from a Possible Service Provider Network

It is assumed that the Mobile IP infrastructure of a service provider consists of many geographically separate networks. We group and name these networks as “Foreign Operation Center”, “Local Operation Center” and “Foreign Networks” as illustrated in Figure 5.1. Foreign Operation Centers are the networks where service provider locates at least one of their AAA servers (Foreign AAA) for domestic use. As we explained before, Foreign AAA servers is used to speed up next authentication of a subscriber and their

existence is not obligatory in terms of Mobile IP standards. Local Operation Center is the core data-house of a service provider. All of the user information stored here with the powerful Home AAA servers and Home Agent servers. Foreign Networks consists of a Foreign Agent and some Mobile Nodes connected to it. They may or may not be correlated with a near Foreign Operation Center. A Foreign Agent can be any kind of active network device whose computational power varies from a wireless access point to a router.

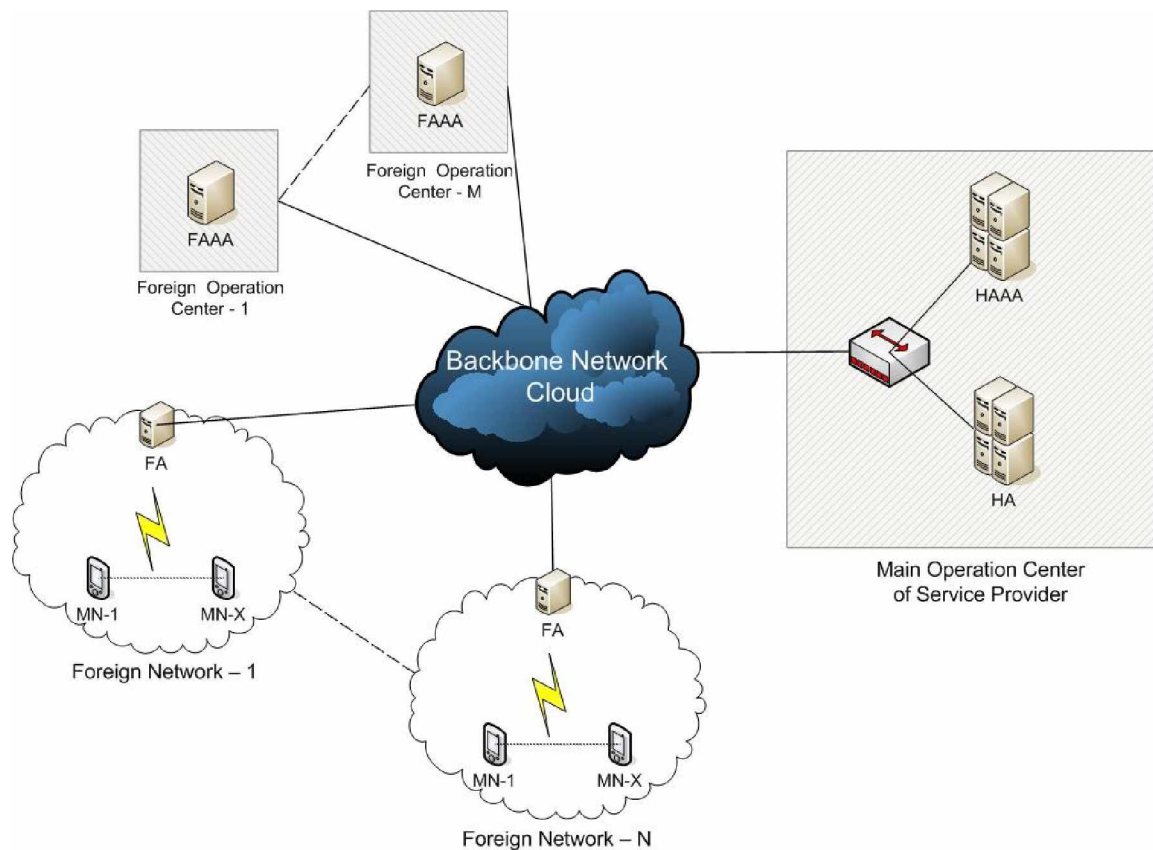


Figure 5.1. An example Service provider network.

This network structure is further simplified for integration to the simulation model. We consider small part of the provided big picture. In the simplified network, illustrated in Figure 5.2, existence of a Main Operation Center with one high-performance Home AAA and Home Agent server is assumed. Furthermore, a group of Foreign Networks and one Foreign Operational Center is defined.

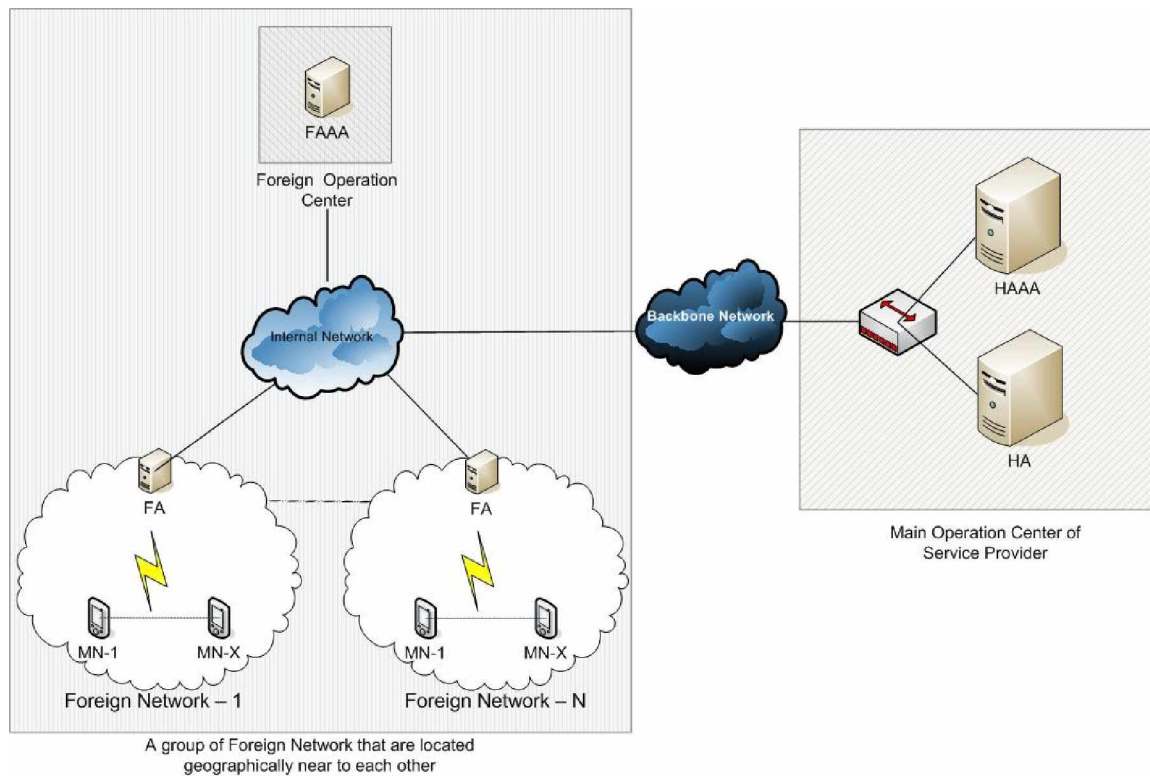


Figure 5.2. Simplified picture of the service provider network.

As last step, we searched similar network models used in Mobile IP with AAA simulation studies [8] and tuned our node numbers accordingly. Our proposed simulation network model, illustrated in Figure 5.3, consist of one Home AAA server connected to one Home Agent, one Foreign AAA server and ten Foreign Agents. Each FA connected to a Mobile Node generator. Mobile Node generator creates increasing number of Mobile Nodes and connects it to corresponding FA. Number of MN created is not limited. Furthermore, generation rate of new MN is increased one per second. In chapter 5.2 we will further explain our simulation environment.

5.1.2. Referenced Computational Costs

As it is explained earlier, for each Mobile IP job there is a constant base computation cost. This cost is found by multiplication of cryptographic operations that occur in corresponding network node and reference time values for each operation in the given hardware architecture.

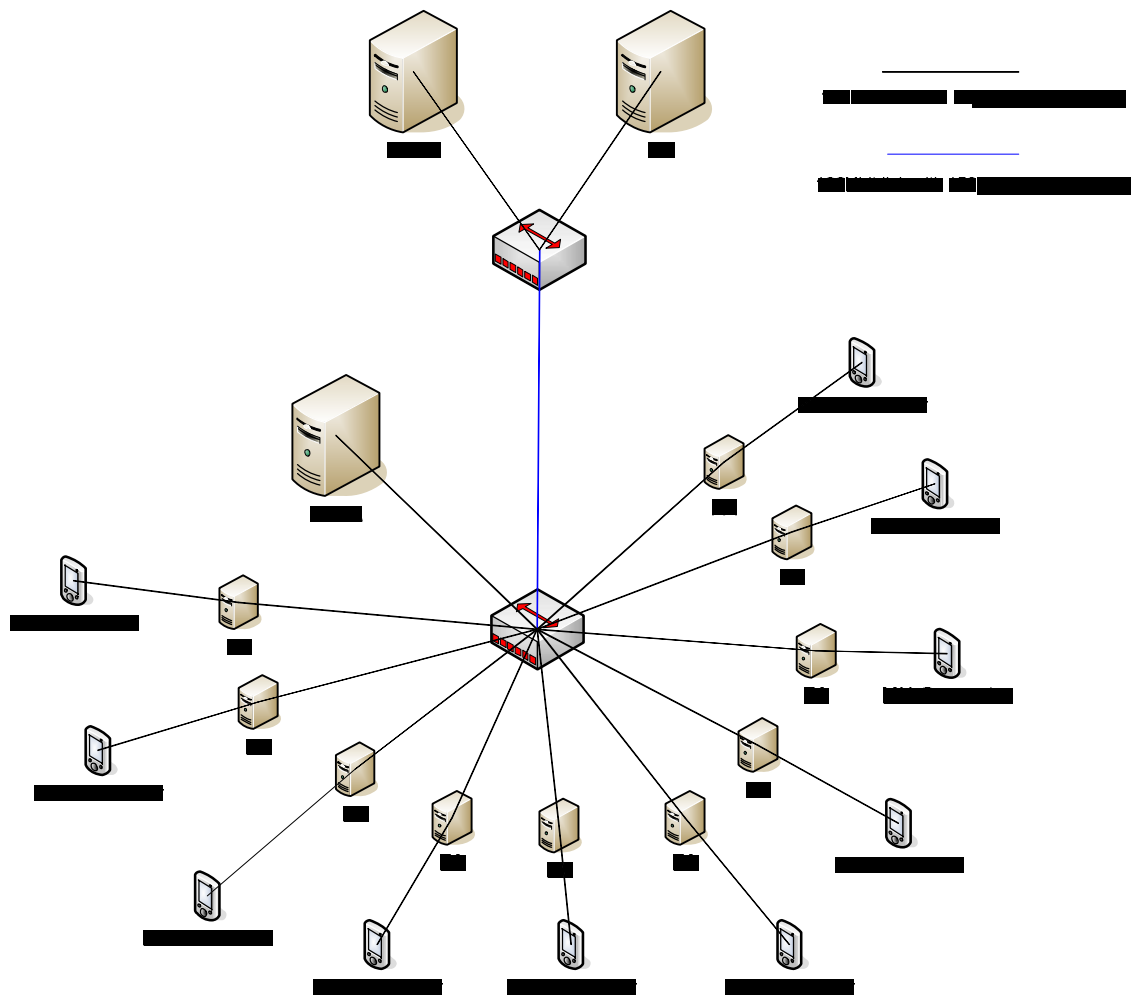


Figure 5.3. Presentation of the simulation network.

Table 5.1. Benchmark results of main hash functions.

Algorithm	MiB/Second	Cycles Per Byte	128 Byte Hashing
MD5	376	6.1	0.32 μ s
SHA-1	216	10.6	0.56 μ s

One of the hardware benchmarks is used for finding the processing times of cryptographic operations, such as MD5, SHA1 (Table 5.1), for a specific processor model, namely AMD Opteron 2.4 GHz processor under Linux 2.6.18 [21]. Same processor model

is used as a server node in the simulation environment. Packets lengths are assumed to be 1024 Bytes and data processed in each hash function assumed to operate on 128 Bytes.

5.1.3. Creating a Job Definition from each Steps of Mobil IP and AAA Communications

We define a job, as a process computed in a network node. In this subchapter, contents of packets sent/received through each step of Mobile IP with AAA communications and processes done on these packets are further identified. Each Mobile IP is presented as $X \Rightarrow Y$, where X is the network node that processes packets to sent Y .

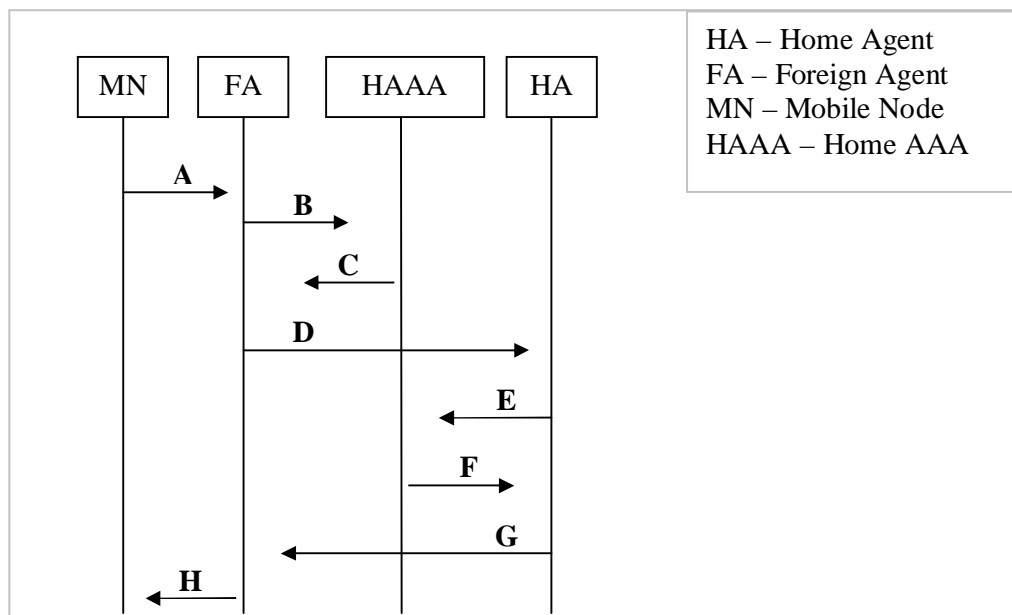


Figure 5.4. Messages of the original Mobile IP and Radius communication.

Packets send in each messaging step of Mobile IP and Radius is illustrated in Figure 5.4. We further specify the cryptographic functions, algorithms used in the source node before creating a message to send. Each computational operation found is correlated to corresponding Mobile IP jobs.

In Message-A, Mobile IP job $MN \Rightarrow FA$, MN forms Registration Request and includes following attributes [6, 22, 23]:

- MN-HA-key-generation-nonce-request
- MN-FA-key-generation-nonce-request
- Challenge extensions
- MN-AAA authentication extension (includes MN-AAA-Authenticator and uses pre-shared MN-HAAA key)

List of cryptographic operations in this Mobile IP job:

- MN-AAA-Authenticator creation.

In Message-B, Mobile IP job FA=>HAA, FA checks the challenge forms RADIUS Access Request [23]: RADIUS-Access Request { User-Name, MIP-MN-HoA, MIP-HA-IP address, MIP-HA-ID, MIP-MA-Type, NAS-ID, MIP-MN-CoA, MIP-MN-FA_Challenge, MIP-HASH-RRQ, MIP-MN-AAA-SPI, MIP-MN-AAA-Authenticator, MIP-feature-vector, Message-Authenticator }.

FA may set the appropriate flags within MIP-feature vector to indicate to the AAAH that it requires keys for FA-MN-MSA and FA-HA-MSA [22]. In our proposal we assume that there is a pre-existing FA-HA-MSA so FA does not ask necessary keys for this association.

List of cryptographic operations in this Mobile IP job:

- MIP-HASH-RRQ creation, as stated in section 5.2 of the draft standard [6].
- Message-Authenticator creation, to sign this transmission as RFC 2869 mandates [24].

In Message-C, Mobile IP job HAAA=>FA, AAAH checks Message-Authenticator, computes and compare own copy of MN-AAA-Authenticator and forms following RADIUS Access Accept: RADIUS Access Accept { User-Name, MIP-MN-HoA, MIP-MA-Type, MIP-HA-IP address (If HA is being delivered by AAA), MIP-HA-ID, MIP-MN-AAA-SPI, MIP-FA-HA-ALGORITHMID, Encrypted (MIP-MN-FA key), MIP-MN-to-FA-SPI, MIP-FA-to-MN-SPI, MIP-MN-FA-Nonce, MIP-MN-FA-MSA-LIFETIME, MIP-MN-FA-ALGORITHMID, Message-Authenticator }

MIP-FA-HA key, MIP-FA-to-HA-SPI, MIP-HA-to-FA-SPI, MIP-FA-HA-MSA-LIFETIME are subtracted from the Access Accept because FA does not request FA-HA-MSA due to its pre-existence. In Message-B, we do not request these values although draft standard shows their existence [6].

List of cryptographic operations in this Mobile IP job:

- Message-Authenticator check, used for checking document integrity as RFC 2869 mandates [24].
- MN-AAA-Authenticator check, used for authenticating MN.
- MIP-MN-FA key generation, as stated in RFC 3957 [22].
- Encrypted MIP-MN-FA key, as “RADIUS Attributes for Tunnel Protocol Support” presents [25]
- Message-Authenticator creation, to sign this transmission.

In Message-D, Mobile IP job FA=>HA, FA checks Message-Authenticator, as RFC 3957 mandates [24] then relays initial Registration Request to HA.

List of cryptographic operations in this Mobile IP job:

- Message-Authenticator check, used for checking document integrity as RFC 2869 mandates [24].
- Foreign-Home Authenticator creation, to sign RRQ transmission as requested

In Message-E, Mobile IP job HA=>HAAA, HA checks Foreign-Home Authenticator. Creates following Radius-Access Request: RADIUS-Access Request { User-Name, MIP-MN-HoA, NAS-ID (HA ID as per RADIUS specification), MIP-MA-Type, MIP-HA-IP address, MIP-FA-IP address, MIP-FA-ID (FA ID as per RADIUS specification), MIP-MN-FA challenge, MIP-MN-AAA-SPI, MIP-MN-AAA-Authenticator, MIP-FA-to-HA-SPI, MIP-HASH-RRQ, MIP-feature-vector, Message_Authenticator }

List of cryptographic operations in this Mobile IP job:

- Foreign-Home Authenticator check, for checking document integrity of the message came from FA.

- MIP-HASH-RRQ creation, as stated in section 5.2 of [6].
- Message-Authenticator creation, to sign this transmission.

In Message-F, Mobile IP job HAAA=>H, AAA checks Message-Authenticator, as mandated in RFC 3957 [24]. HAAA checks MN-AAA-Authenticator to validate the request and creates the MN-HA key and the corresponding nonces for MN-HA MSAs and creates following RADIUS Access Accept: RADIUS Access Accept {User-Name, MIP-MN-HoA, MIP-MA-Type, MIP-HA-IP address, MIP-HA-ID, Encrypted (MIP-MN-HA key), MIP-MN-to-HA SPI, MIP-HA-to-MN-SPI, MIP-MN-HA-Nonce, MIP-MN-HA-ALGORITHMID, MIP-MN-HA-REPLAY, MIP-MN-HA-MSA-LIFETIME, MIP-MN-FA-Nonce, MIP-MN-FA-ALGORITHMID, MIP-MN-FA-REPLAY, MIP-MN-FA-MSA-LIFETIME, Message-Authenticator}.

MIP-FA-HA key, MIP-FA-to-HA-SPI, MIP-HA-to-FA-SPI, MIP-FA-HA-ALGORITHMID, MIP-FA-HA-MSA-LIFETIME are subtracted parts due to pre-existence of FA-HA-MSA. In Message-E we do not request these values although draft document shows their existence [6].

List of cryptographic operations in this Mobile IP job:

- Message-Authenticator check, used for checking document integrity as RFC 2869 mandates [24].
- MN-AAA-Authenticator check, for authenticating MN
- MIP-MN-HA key generation, as stated in RFC 3957 [22].
- Encrypted MIP-MN-HA key, as “RADIUS Attributes for Tunnel Protocol Support” presents [25].
- Message-Authenticator creation, to sign this transmission.

In Message-G, Mobile IP job HA=>FA, HA checks Message-Authenticator, as RFC 2869 mandates [24]. The HA processes the RRQ and builds a Mobile IP registration reply.

List of cryptographic operations in this Mobile IP job:

- Message-Authenticator check, used for checking document integrity as RFC 2869 mandates [24].
- Foreign-Home Authenticator creation, to sign RRP transmission.

In Message-H, Mobile IP job FA=>MN, FA relays Registration reply to MN.

List of cryptographic operations in this Mobile IP job:

- Foreign-Home Authenticator check, used for checking document integrity as RFC 2869 mandates [24].

In Message-I, Mobile IP job MN=>MN, MN creates MN-HA and MN-FA keys with incoming nonces.

List of cryptographic operations in this Mobile IP job:

- MIP-MN-HA key generation, as explained in RFC 3957 [22].
- MIP-MN-FA key generation, as explained in RFC 3957 [22].

5.1.4. Calculating the Base Processing Time for Mobile IP Jobs

In this subsection details of each cryptographic operation listed in previous section is explained. After identifying each operation we provide total number of hash functions used in each job and calculate the processing time for each job.

MN-AAA-Authenticator is prepared by MN as defined in Message-A. It is recalculated by HAAA server in Message-C, Message-F. MIP-HASH-RRQ is pre-calculated value for decreasing number of extensions.

$$\text{Authenticator} = \text{MD5}(\text{High-order byte from Challenge} \parallel \text{Key} \parallel \text{Value of MIP-HASH-RRQ} \parallel \text{Least-order 237 bytes from Challenge}) \quad (5.1)$$

RFC 2869 mandates usage of Message-Authenticator in every RADIUS message signaling [24]. Sender will calculate and put it in message, receiver will recalculate the value. It is used in message Message-B, Message-C, Message-E, and Message-F.

$$\text{Message-Authenticator} = \text{HMAC-MD5} (\text{Type, Identifier, Length, Request Authenticator, Attributes}) \quad (5.2)$$

The AAA server uses the value of MIP-HASH_RRQ to calculate the authenticator in MN-AAA Authenticator. This is created by FA as defined in Message-B and by HA in Message-E.

$$\text{MIP-HASH-RRQ} = \text{MD5} (\text{RRQ}) \quad (5.3)$$

MIP-MN-FA key generation / MIP-MN-HA key generation process is done by HAAA as defined in Message-C and Message-B and MN in Message-I.

$$\text{Key} = \text{HMAC-SHA1} (\text{AAA-key, \{Key Generation Nonce || mobile node identifier\}}) \quad (5.4)$$

RADTUNN is used for encrypting keys (MIP-MN-HA, MIP-MN-FA) with a shared secret. Methodology is described in [25]. It consists of n MD5 operations where n is calculated by $\text{length} * (\text{Plaint text}) / 16$. In our case we are assuming 128bit password length so cost of this operation will be $128/16=8$ MD5 operations.

HMAC is a combination of mathematical operations with 2 Hash functions. Methodology is defined in [26].

Summarization of job processing times can be found in Table 5.2. Operations done in jobs and total hashing operations are listed. Processing time of the jobs found by multiplication of total number of hash functions with cryptographic operation times listed in Table 5.1.

5.1.5. Event Sequence of Current Approach in Mobile IP

The simulation model of current approach includes all the steps defined in Mobile IP standard [6]. After Registration Request (RRQ) made by Mobile Node. Following events occur simultaneously:

Table 5.2. Summary of Mobile IP job processing times.

Job Name	Operations Done	Number of Hash Operations	Processing time of the Job
MN => FA	MN-AAA-Authenticator creation	1 MD5	0.32 μ s
FA=>HAAA	MIP-HASH-RRQ creation Message-Authenticator creation	3 MD5	1.6 μ s
HAAA => FA	Message-Authenticator check MN-AAA-Authenticator check MIP-MN-FA key generation MIP-MN-FA key Message-Authenticator creation	13 MD5 2 SHA1	5.28 μ s
FA => HA	Message-Authenticator check Foreign-Home Authenticator creation	4 MD5	1.28 μ s
HA => HAAA	Foreign-Home Authenticator check MIP-HASH-RRQ creation Message-Authenticator creation	5 MD5	1.6 μ s
HAAA => HA	Message-Authenticator check MN-AAA-Authenticator check MIP-MN-HA key generation Encrypted MIP-MN-HA key Message-Authenticator creation	13 MD5 2 SHA1	5.28 μ s
HA => FA	Message-Authenticator check Foreign-Home Authenticator creation	4 MD5	1.28 μ s
FA => MN	Foreign-Home Authenticator check	2 MD5	0.64 μ s
MN	MIP-MN-HA key generation MIP-MN-FA key generation	4 SHA1	2.24 μ s

- FA creates an RADIUS Access Request message (AReq) and sends this message to its AAA server (FAAA).
- Foreign AAA process and forward request to Home AAA.

- Home AAA server processes this request and creates RADIUS Access Accept/Deny message (ARep) and sends it back to Foreign AAA.
- Foreign AAA forwards the RADIUS Access Accept/Deny message (ARep) to Foreign Agent (FA).
- Foreign Agent (FA) confirms that Mobile Node (MN) is authenticated. Then it creates Registration Request (RRQ) and sends it to Home Agent (HA).
- After receiving Registration Request (RRQ), to authenticate Mobile Node (MN) and take necessary key and challenges for creating Mobil Secure Association (MSA), Home Agent (HA) sends Access Request message (AReq) to Home AAA server.
- Home AAA server sends corresponding Access Response to Home Agent (HA).
- Home Agent (HA) creates Registration Reply (RRP) message, to show registration result, and sends to Foreign Agent (FA).

In last step, communication flow ends with primary event; Foreign Agent (FA) forwards Registration Reply (RRP) to Mobile Node (MN). In chapter 5.1.2, process time for each of these communications is given.

5.1.6. Event Sequence of Simulation Model of Proposed Approach

The simulation model of proposed approach includes all the steps defined in Mobile IP standard [6]. After Registration Request (RRQ) made by Mobile Node. Following secondary events occur:

- Foreign Agent (FA) creates an RADIUS Access Request message (AReq) to its AAA server (FAAA). Simultaneously, Foreign Agent (FA) creates RRQ and sends it to Home Agent (HA).

After this event, two branches of events occur simultaneously. Branch-1 goes on as follows:

- Foreign AAA forward request to Home AAA server.

- Home AAA server authenticates MN it creates RADIUS Access Accept/Deny message (ARep) and sends it back to FAAA.
- Foreign AAA server forwards the RADIUS Access Accept/Deny message (ARep) to Foreign Agent (FA).

In parallel Branch-2 continue with following sequence:

- After receiving RRQ HA, to authenticate MN and take necessary key and challenges for creating MSA from HAAA, sends AReq to Home AAA server.
- Home AAA server sends corresponding Access Response to Home Agent (HA).
- Home Agent (HA) creates Registration Reply (RRP) message, to show registration result, to Foreign Agent (FA).

Then in last step, when both Foreign AAA server and Home Agent (HA) responses arrive to Foreign Agent (FA), FA forwards Registration Reply (RRP) to Mobile Node (MN). In chapter 5.1.2, process time for each of these communications is given.

5.2. Our Simulation Environment: OPNET

In this subchapter we will give details about our simulation tool OPNET and we will provide the network created and configurations used.

OPNET is a well known discrete event simulator referenced in many articles. It is also been preferred by simulation researches on Mobile IP subject [4, 5]. It is a multipurpose simulation environment with many distinct modules that enables researcher to use most of the current technologies, products, protocols in various details. In our work we used especially “Server Characterization Editor” module to create a realistic service provider data-house structure with real server models currently used in service providers. We are able to detail each Mobile IP process’s costs on the system by giving each process CPU, Memory and disk I/O usage. By this module we are also able to apply several computational powers to each network nodes to see the interaction of distinct types of network structures with current and proposed approach.

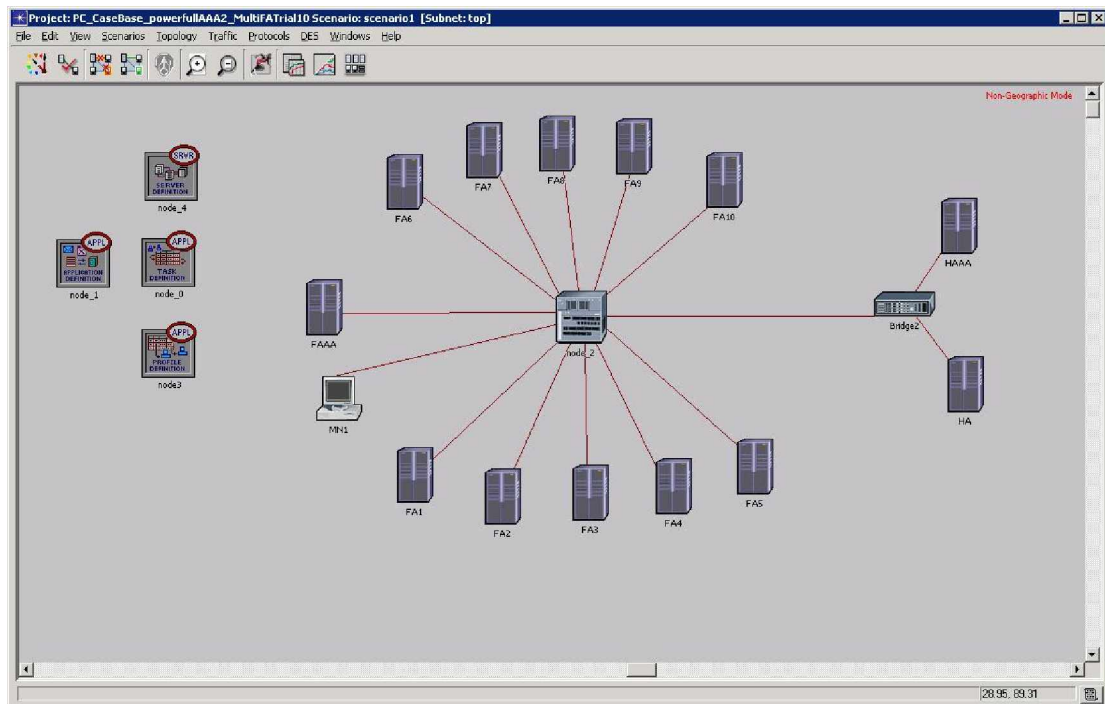


Figure 5.5. OPNET network structure.

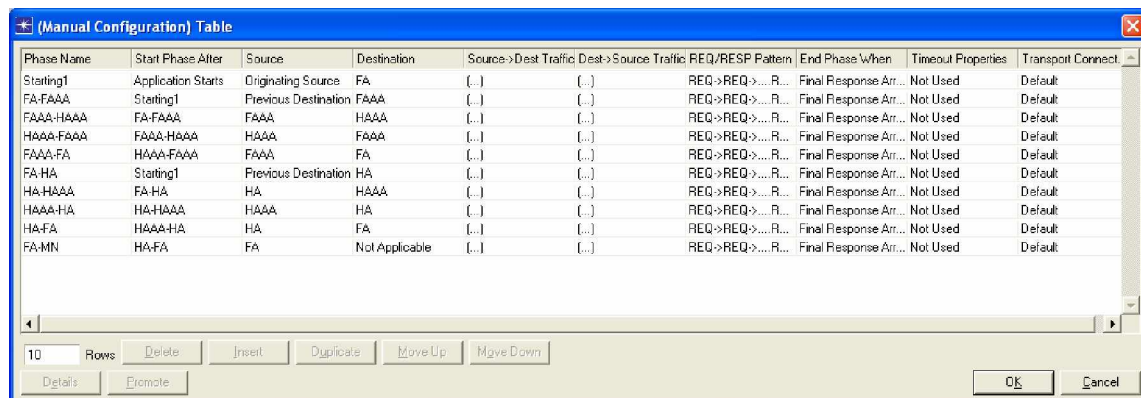
5.2.1. Network Scheme Created in OPNET

We created a network structure (Figure 5.5) that models the simplified Mobile IP network described in section 5.1.1 (Figure 5.3). There are 10 Foreign Agent nodes connected to a MN generator (MN1 in the Figure 5.5) and a Foreign AAA server through a bridge (switch). At the other side of the network there is a Home AAA server and Home Agent that is connected via a bridge. The link between these two bridges represents the inter domain connection. The other links represent inner domain connections.

5.2.2. Setting Job Processing Time in OPNET

Mobile node generator initiates tasks and assigns them to each Foreign Agent Nodes sequentially. Each task initiates other tasks or communication through the network. Figure 5.6 shows the OPNET task configuration for our Mobile IP registration approach. Each task represents a Mobile IP job defined in section 5.1.3. This sequential relation of tasks through the network simulates the Mobile IP protocol processing. A sequence of a

Mobile IP tasks ends at in the initial point, the Mobile IP generator. The time between start and end of this communication shows the Mobile IP registration time of the node.



Phase Name	Start Phase/Alter	Source	Destination	Source->Dest Traffic	Dest->Source Traffic	REQ/RESP Pattern	End Phase/When	Timeout Properties	Transport Connect
Starting1	Application Starts	Originating Source	FA	(...)	(...)	REQ->REQ->... R...	Final Response Arr...	Not Used	Default
FA-FAAA	Starting1	Previous Destination	FAAA	(...)	(...)	REQ->REQ->... R...	Final Response Arr...	Not Used	Default
FAAA-HAAA	FA-FAAA	FAAA	HAAA	(...)	(...)	REQ->REQ->... R...	Final Response Arr...	Not Used	Default
HAAA-FAAA	FAAA-HAAA	HAAA	FAAA	(...)	(...)	REQ->REQ->... R...	Final Response Arr...	Not Used	Default
FAAA-FA	HAAA-FAAA	FAAA	FA	(...)	(...)	REQ->REQ->... R...	Final Response Arr...	Not Used	Default
FA-HA	Starting1	Previous Destination	HA	(...)	(...)	REQ->REQ->... R...	Final Response Arr...	Not Used	Default
HA-HAAA	FA-HA	HA	HAAA	(...)	(...)	REQ->REQ->... R...	Final Response Arr...	Not Used	Default
HAAA-HA	HA-HAAA	HAAA	HA	(...)	(...)	REQ->REQ->... R...	Final Response Arr...	Not Used	Default
HA-FA	HAAA-HA	HA	FA	(...)	(...)	REQ->REQ->... R...	Final Response Arr...	Not Used	Default
FA-MN	HA-FA	FA	Not Applicable	(...)	(...)	REQ->REQ->... R...	Final Response Arr...	Not Used	Default

Figure 5.6. OPNET task configuration.

5.2.3. Automatic Scaling of Job Resource Consumption

Each task has their own system resource cost on the node it is processed. This cost is defined for one type of a server structure. We calculated our tasks for a specific hardware in section 5.1.3. After correlating each task cost with one type of server hardware, OPNET allows you easily use new server structures without manual calculation and configuration. It is able to calibrate the new costs according to new hardware that is used. For example, in Figure 5.7 an Average CPU time is set for the job in a 2800 MHz AMD Opteron environment. After defining its resource consumption details for a given system we can assign this job to any hardware with various computational powers. For example, in Figure 5.8 we assign the job, that we create above, to a SUN Fire server environment with 8 900 MHz CPUs. OPNET, automatically, scales the input parameters given in the job definition for the new environment and calculates new resource costs for this hardware.

By this useful property we are able to run our simulation in different computational power environments and compare the results without concern of exact scaling.

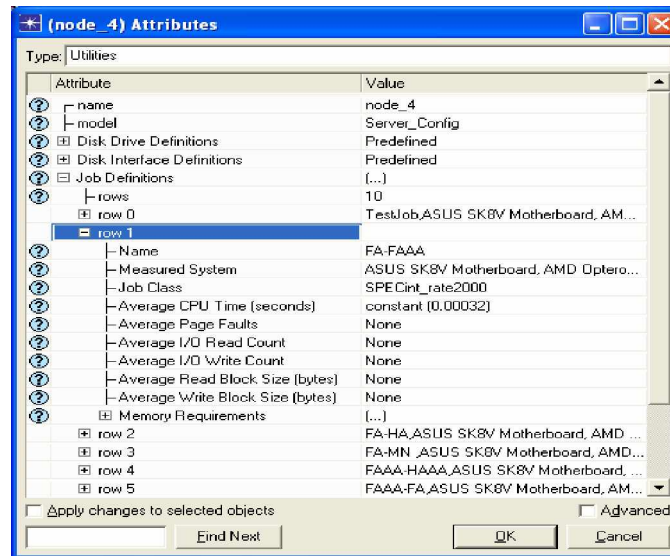


Figure 5.7. Setting a process cost to server hardware in OPNET.

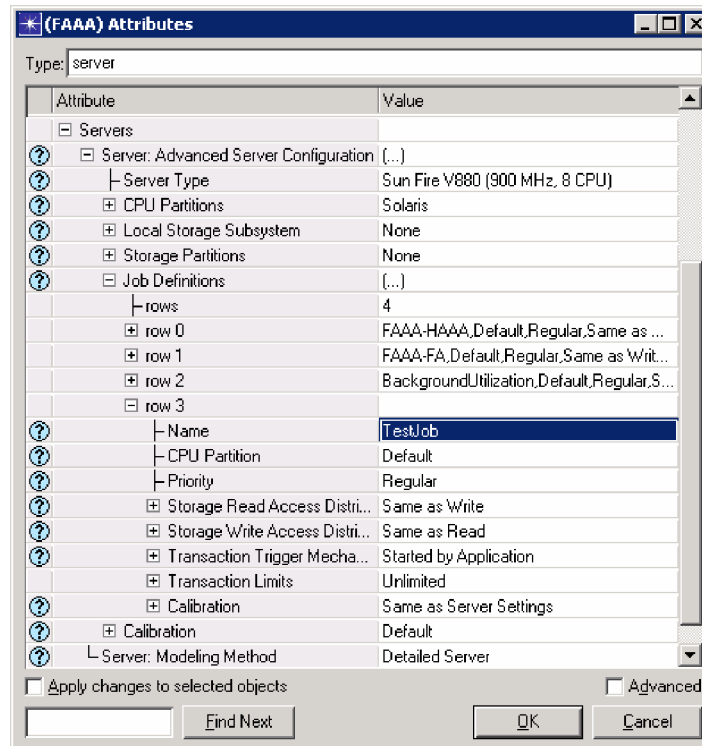


Figure 5.8. Assigning a job to server hardware in OPNET.

5.3. List of Input Sets Simulated

After creating simulation environment as described in subchapter 5.2 we applied different input values to test the system performance in various conditions. In this subchapter we will explain the different set of inputs used. For each input sets we ran the simulation twice. One is for current practice of ‘Mobile IPv4 with Radius’ as described in subsection 2.2 and other one is for our proposed solution ‘Parallel Mobile IP and Radius’ as described in section 3.

5.3.1. Link Delays Simulated

For Mobile IP registration process, link speeds always be a critical value. The importance of inner and inter domain communication time are been underlined in very first standards about the subject [7]. As we also argued through this thesis rather than computational complexity of the registration processes, domain communication is most important reason for the delays in overall registration. Especially inter domain communication has an important effect because of its delay when compared to other costs.

To analyze the systems behavior on different link speed we test the following set of link delay values for inner and inter domain communications;

- 10 ms inner domain, 100 ms inter domain.
- 10 ms inner domain, 300 ms inter domain.
- 10 ms inner domain, 500 ms inter domain.
- 10 ms inner domain, 700 ms inter domain.
- 30 ms inner domain, 100 ms inter domain.
- 30 ms inner domain, 300 ms inter domain.
- 30 ms inner domain, 500 ms inter domain.
- 30 ms inner domain, 700 ms inter domain.
- 50 ms inner domain, 100 ms inter domain.
- 50 ms inner domain, 300 ms inter domain.
- 50 ms inner domain, 500 ms inter domain.

- 50 ms inner domain, 700 ms inter domain.

For all the sets above, same hardware settings used. For FAs SUN Ultra 10 (333 MHz), for Servers (FAAA, HAAA, HA) Sun Fire v880 (900 MHz, 8 CPU) is used.

5.3.2. Network Node Hardware Simulated

When the Mobile IP started to be deployed, in real environment, there will be various hardware choices. ISP's may use their current datawarehouse servers or invest in different solutions. On the other hand, at the customer side, there can be different foreign agent hardware. Nowadays, most of the enterprise routers support Mobile IP, there are software solutions that can be run on any server/pc and there are different wireless base transceiver stations from WiFi access points to Node Bs of 3G cellular networks.

To analyze the behavior of Mobile IP system in this variable environment we test our solution and current practice on following hardware;

- FAs as Sun Ultra 10 (333 MHz), Servers as Sun Fire v880 (900 MHz, 2 CPU).
- FAs as Sun Ultra 10 (333 MHz), Servers as Sun Fire v880 (900 MHz, 4 CPU).
- FAs as Sun Ultra 10 (333 MHz), Servers as Sun Fire v880 (900 MHz, 8 CPU).
- FAs as Sun Fire V880 (750 MHz), Servers as Sun Fire v880 (900 MHz, 8 CPU).
- FAs as Sun Fire V240 (1.28 GHz), Servers as Sun Fire v880 (900 MHz, 8 CPU).

For all the sets above, same link speed is used. For inner domain communications 30ms, for inter domain communications 500ms is used.

5.3.3. Network Node Background Utilizations Simulated

As we described in subchapter 5.3.2, we expect to have various transceiver and datacenter hardware profiles. On the other hand, this server, transceiver boxes probably will be running other tasks or protocols parallel to Mobile IP. At the server point of view, for example, we can expect an ISP to run one AAA server structure and link any AAA using infrastructure to this base AAA server(s). At the transceiver point of view, for

example, we can expect a GSM transceiver basically to run GSM protocols as its normal workload. These mean that our Mobile IP protocol will be running on boxes where there are high or low background utilizations.

To analyze the behavior of Mobile IP system in this variable background utilized environment we test our solution and current practice on following hardware settings;

- FAs as Sun Ultra 10 (333 MHz), Servers as Sun Fire v880 (900 MHz, 8 CPU) with %50 background utilization.
- FAs as Sun Ultra 10 (333 MHz), Servers as Sun Fire v880 (900 MHz, 8 CPU) with %75 background utilization.
- FAs as Sun Fire V240 (1.28 GHz) with %73.984375 background utilization, Servers as Sun Fire v880 (900 MHz, 8 CPU).
- FAs as Sun Fire V240 (1.28 GHz) with %41.40625 background utilization, Server as Sun Fire v880 (900 MHz, 8 CPU).

For all the sets above, same link speed is used. For inner domain communications 30ms, for inter domain communications 500ms is used.

5.4. Simulation Results

Through the simulations we expected to figure out registration time and scalability performances of both approaches in different environment settings. For this purpose we categorize the simulation results in two main subchapters; registration time and system scalability. In each subchapter we further explain outcome of the simulation sets given in subchapter 5.3.

In all of the simulation runs we had to scale the system in 1/1000 ratio to speed up the simulation speed. The computational costs of Mobile IP processes that are described and calculated in section 5.1.4 are in microseconds for a given hardware. This low cost enables similar hardware to handle million of Mobile IP jobs in a second. Simulating hardware that process million jobs in a seconds creates a high resource burden on our simulation computers. To ease the situation and fulfill the memory and CPU requirements of this

simulation process we scaled the computational costs of each Mobile IP job 1000 times. We defined each process time in milliseconds rather than microseconds. By this modification we expect to have the results that are presenting 1000 times less Mobile IP active job/request numbers. All the graphs, findings that will be shown below are bare results. To achieve the real values number of Mobile IP active job/request numbers must be multiplied with 1000. In conclusion chapter of this thesis, when these results are discussed, 1000 times greater values will be used.

5.4.1. Overall Registration Time Results of Both Approaches

5.4.1.1. Effect of Link Delays. Figures from 5.9 to 5.11 represent overall registration time performance of current practice of Mobile IP. Each graph represents affect of different inter communication delays under 10ms, 30ms, 50ms inner communication delays.

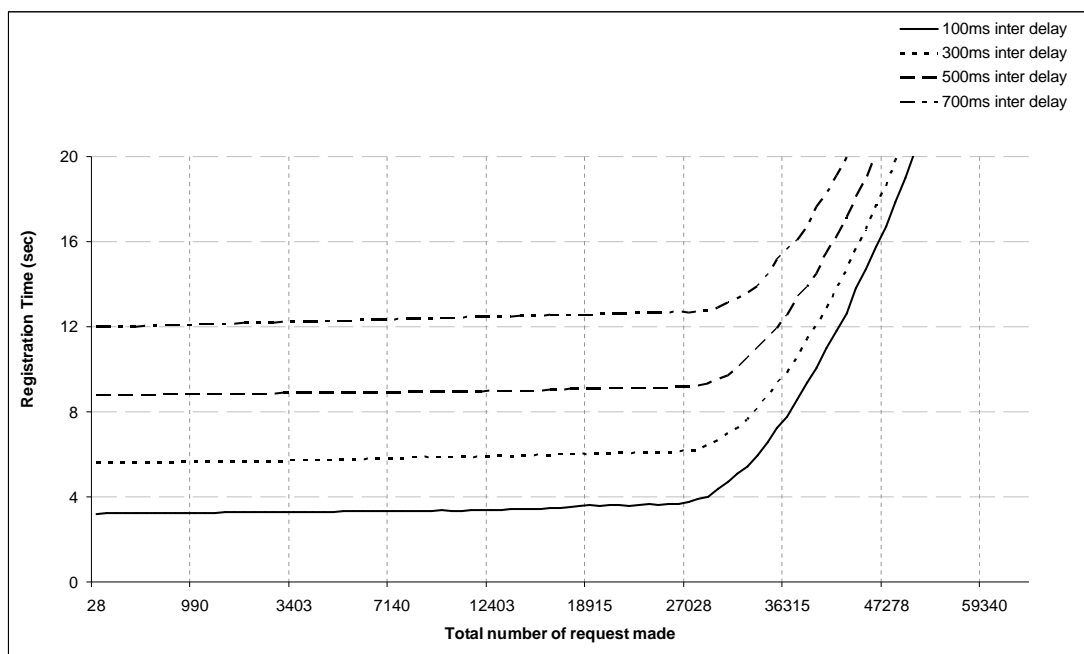


Figure 5.9. Registration speed of the current practice under 10 ms inner communication delay

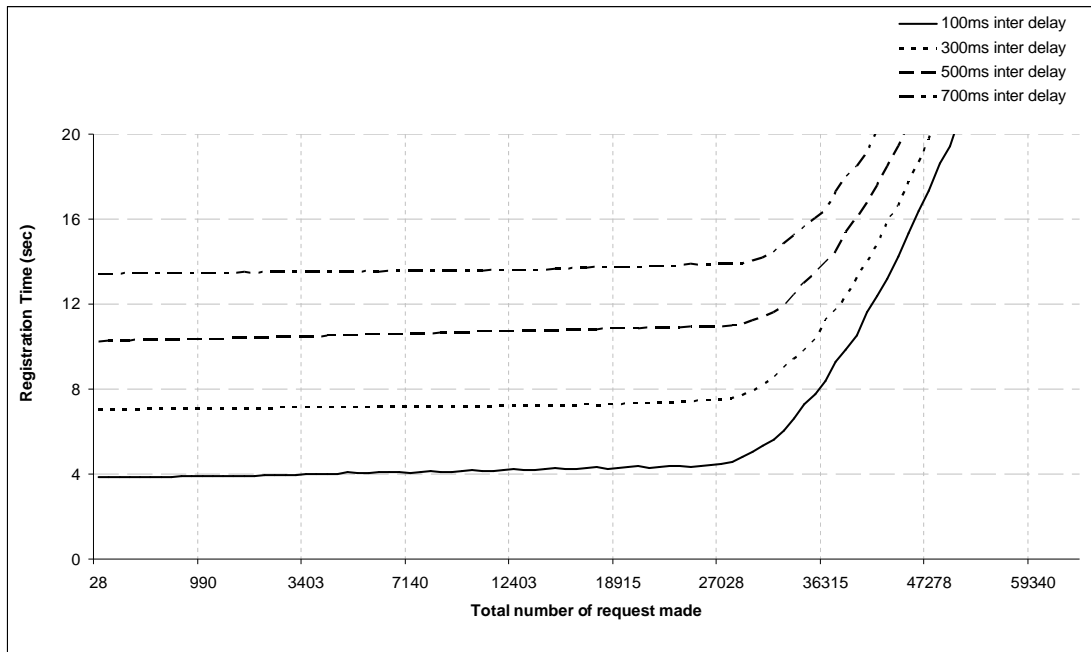


Figure 5.10. Registration speed of the current practice under 30 ms inner communication delay

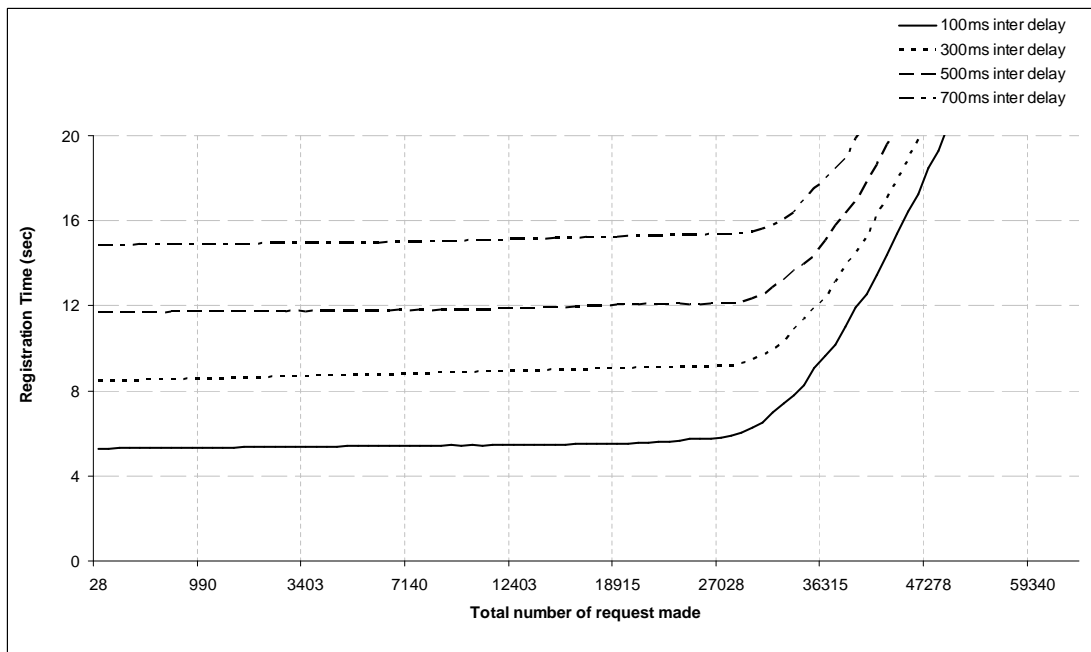


Figure 5.11. Registration speed of the current practice under 50 ms inner communication delay

In three figures when we compare 100-700 ms delay graphs we can see that when the inter communication delay rise seven times, the overall registration increase more than three times. For example let's examine the values of Figure 5.10. The overall registration with 100 ms inter domain delay simulation gives approximately 4 sec till total registration request are less than 20,000. In same figure, for same time period, 700 ms inter delay gives approximately 13.6 sec. This shows that inter delays have very critical affect on registration time.

Figures from 5.12 to 5.14 represent overall registration time performance of our solution of Mobile IP. Each graph represents affect of different inter domain communication delays under 10 ms, 30 ms, 50 ms inner communication delays.

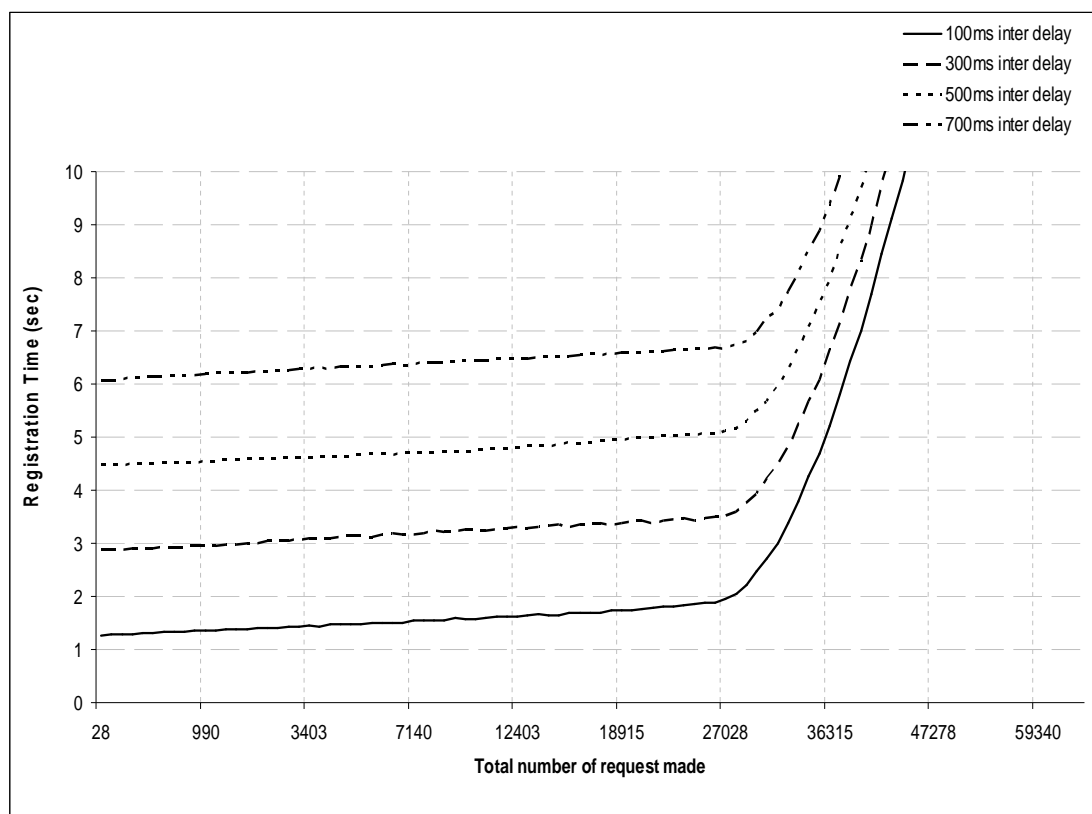


Figure 5.12. Registration speed of the proposed solution under 10 ms inner communication delay

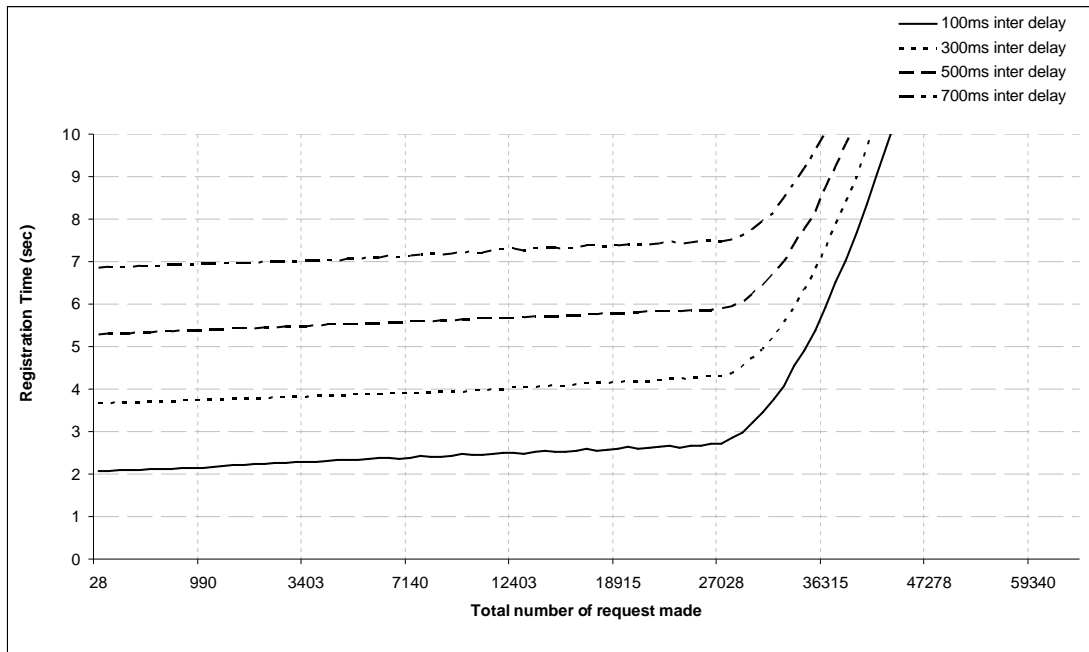


Figure 5.13. Registration speed of the proposed solution under 30 ms inner communication delay

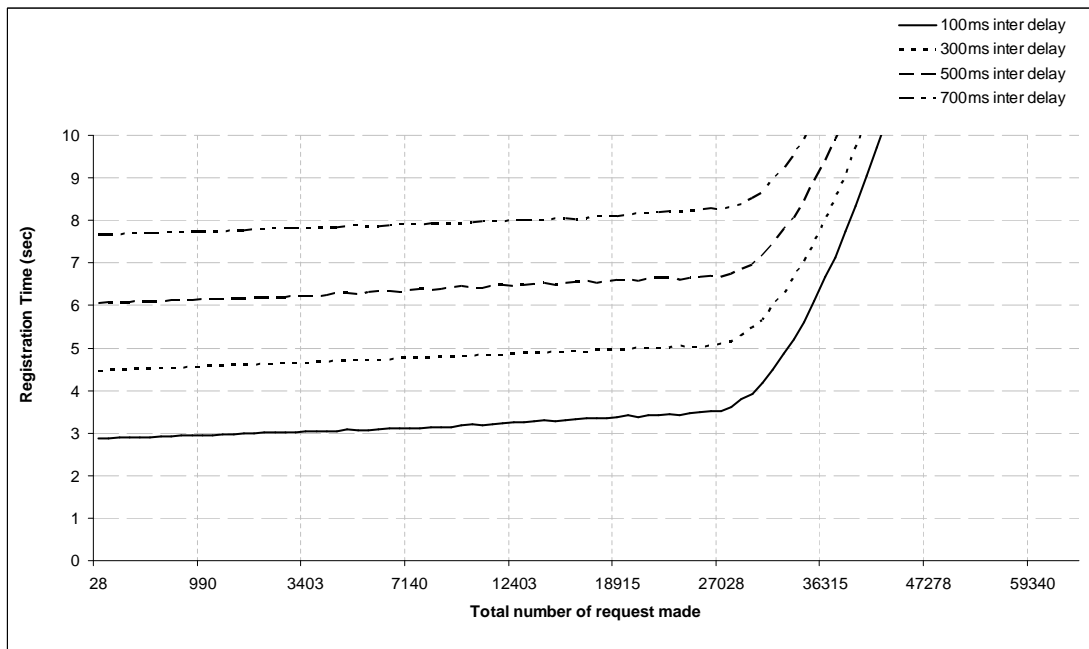


Figure 5.14. Registration speed of the proposed solution under 50 ms inner communication delay

When we compare our solution's graphs with current approach in three graphs we see that our solution gives nearly two times faster registration performance. For example let's examine the Figures 5.14 and 5.11. For 100 ms inter delay our solution gives 2.86 sec, current approach gives 5.29 sec for registration time. The ratio is 1.85. Our solution is 1.85 times faster. When we increase the inter communication delay, as we mentioned in analytical analysis section, our solution start to perform better. In the Figure 5.14 and 5.11 we can see that for 700 ms inter delay our solution gives 7.6 sec, current approach gives 14.8 sec for registration time. The ratio is 1.94. As we mentioned before, this ratio will approach to 2 when the difference between inter and inner delay grow bigger.

Figures from 5.15 to 5.18 represent overall registration time performance of current practice of Mobile IP. Each graph represents affect of different inner communication delays under 100ms, 300ms, 500ms, 700ms inter communication delays.

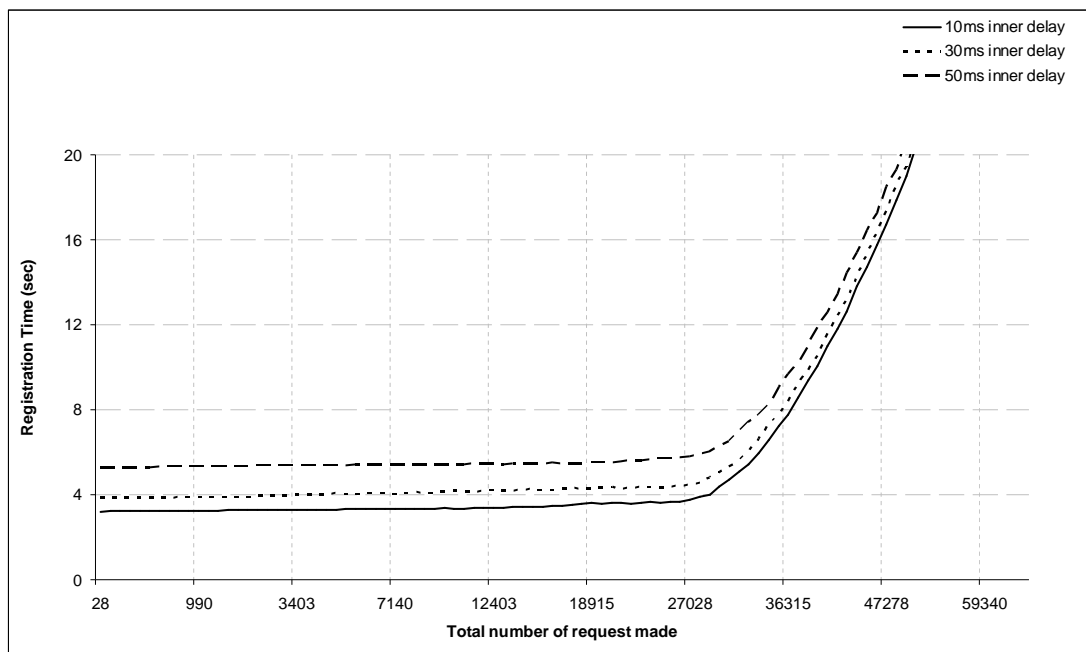


Figure 5.15. Registration speed of the current practice under 100 ms inter communication delay

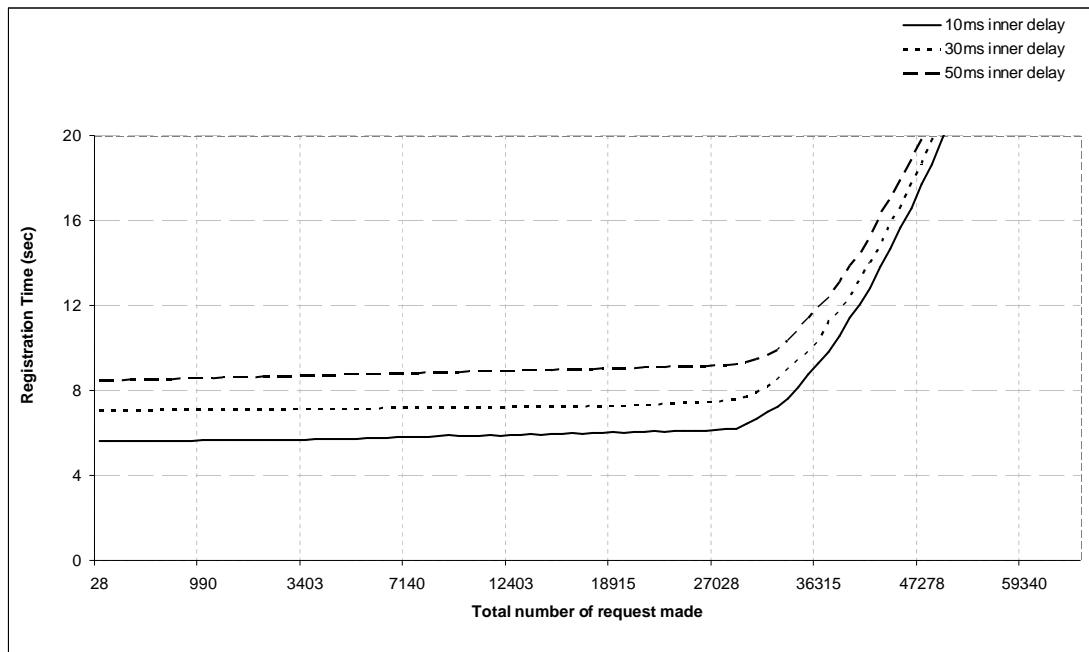


Figure 5.16. Registration speed of the current practice under 300 ms inter communication delay

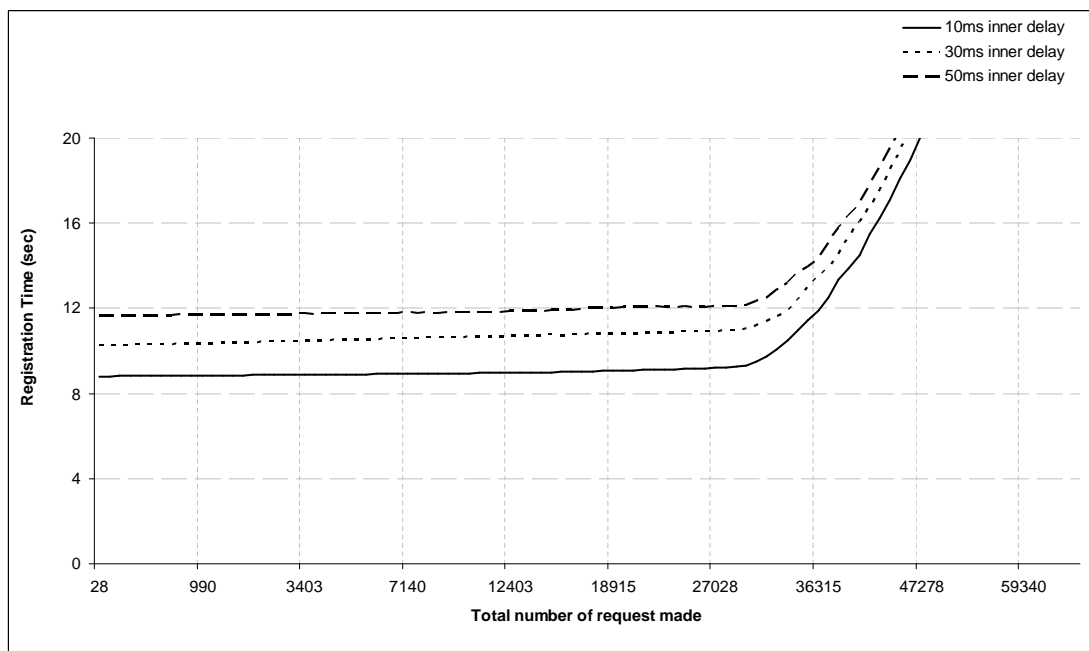


Figure 5.17. Registration speed of the current practice under 500 ms inter communication delay

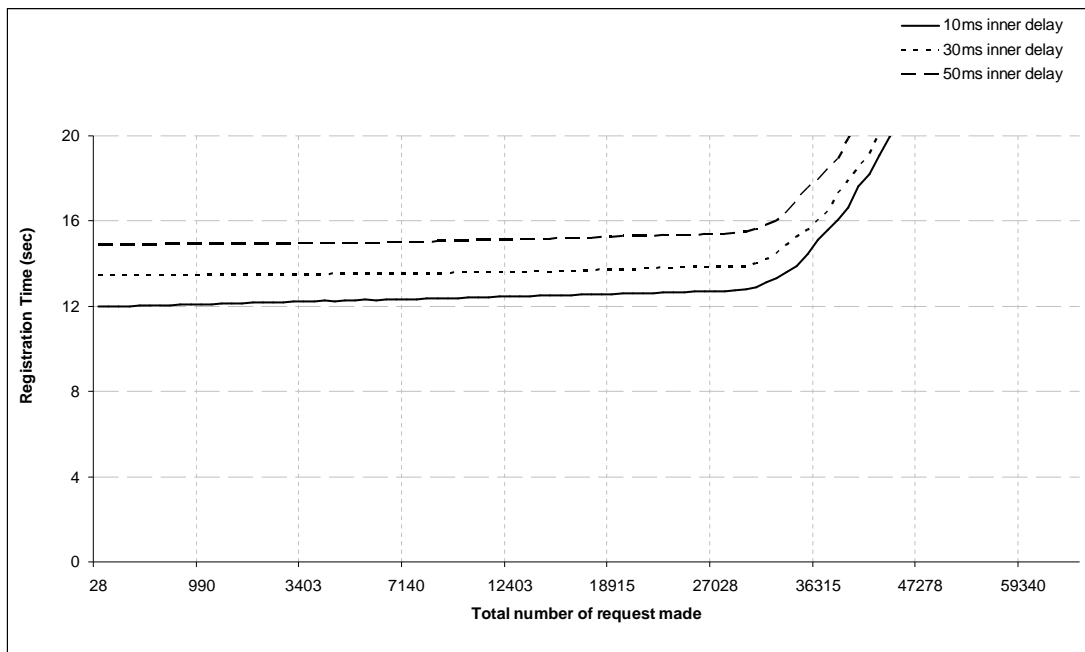


Figure 5.18. Registration speed of the current practice under 700 ms inter communication delay

When we count number of inter communications and compare with inner communications we see that there is always more inner communication occurring. So if the inner delays were high as inter delays they will be more affective. But inner communication delays are much less than inter communication delays because they represents near hops in a multi-hop network. So their overall addition to registration time becomes less important when other major costs like inter delays become bigger. For example, let’s compare Figures 5.15 and 5.18. In 100 ms inter communication delay the 50 ms inner delay generates 5.3 sec, 10 ms inner delay generates 3.2 sec registration time. The ratio is 1.625. When we start to increase the inter communication delay to 700 ms we see that the 50 ms inner delay produce 14.8 sec, 10 ms inner delay produce 12 sec registration time. In this case the ratio is 1.23. So this shows that when inter delays affect grow bigger inner delay affect become more negligible.

Figures from 5.19 to 5.22 represent overall registration time performance of our solution of Mobile IP. Each graph represents affect of different inner communication delays under 100ms, 300ms, 500ms, 700ms inter communication delays.

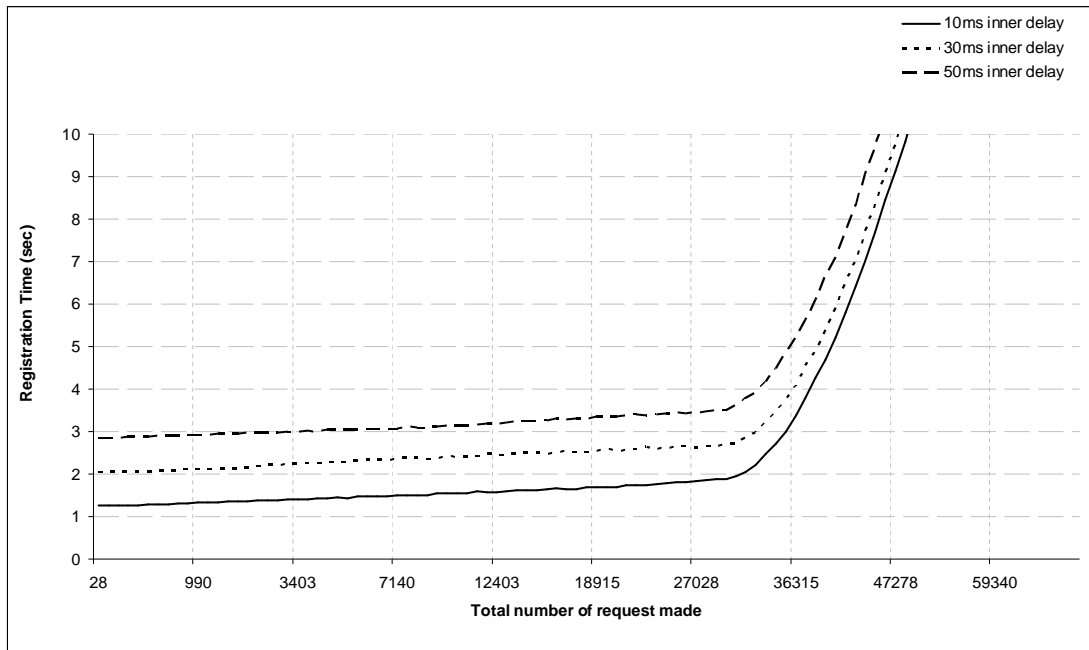


Figure 5.19. Registration speed of the proposed solution under 100 ms inter communication delay

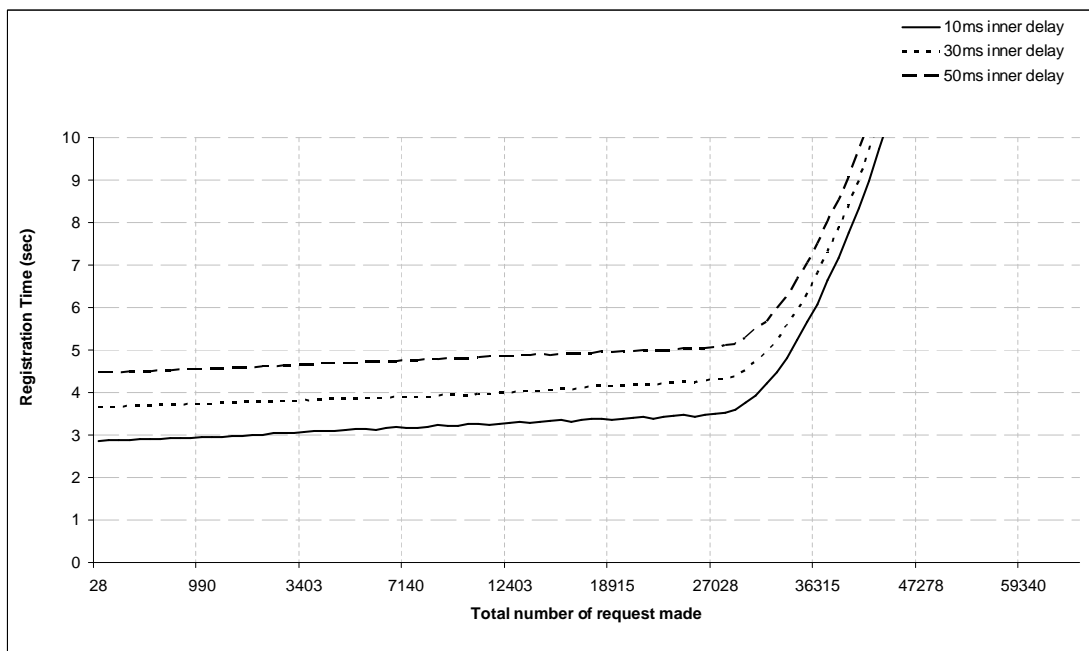


Figure 5.20. Registration speed of the proposed solution under 300 ms inter communication delay

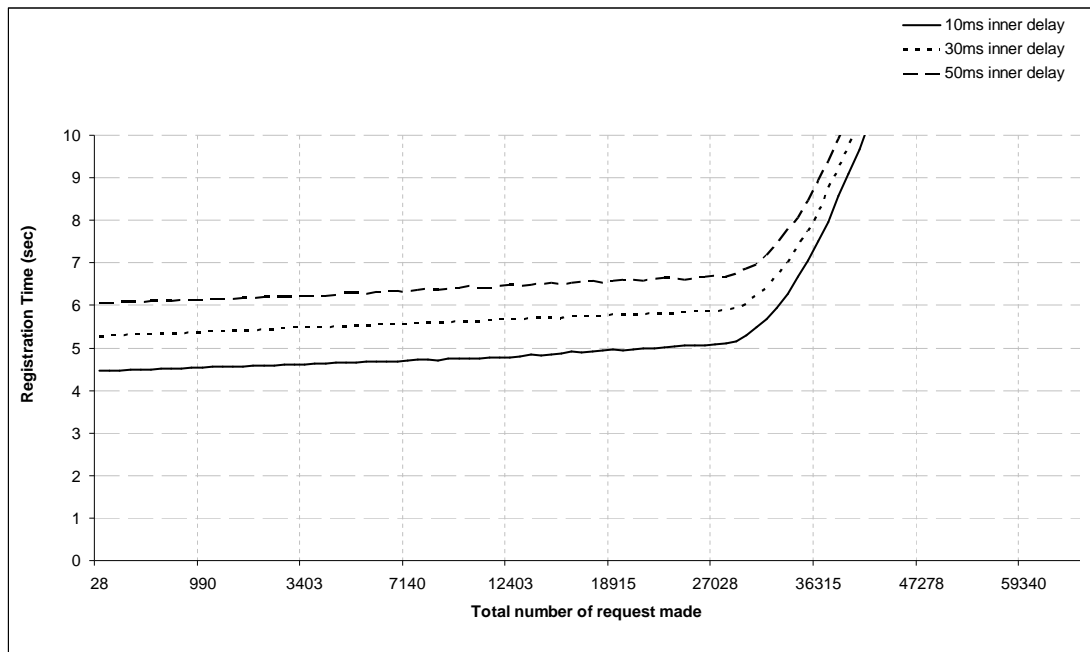


Figure 5.21. Registration speed of the proposed solution under 500 ms inter communication delay

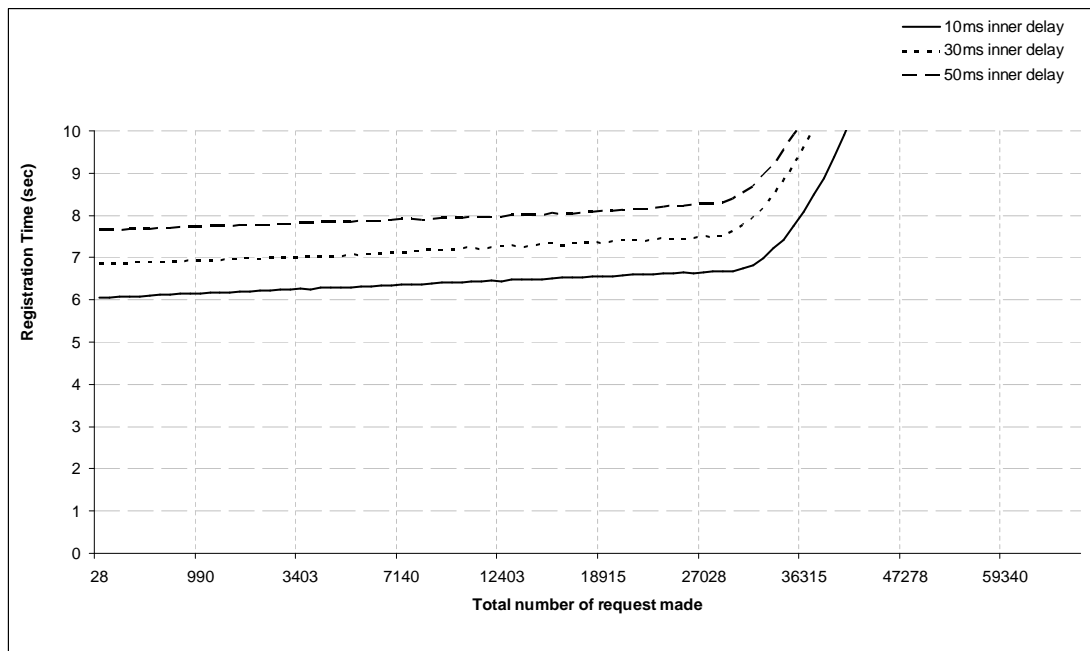


Figure 5.22. Registration speed of the proposed solution under 700 ms inter communication delay

When we compare our solution performance with current practice by inter communication delay figures above. We again achieve the same result that shows our solution is nearly two times faster than current practice. For example, let's compare Figures 5.19 and 5.22 with 5.14 and 5.18. For 100 ms inter and 50 ms inner delays our solution gives 2.86 sec, current practice gives 5.29 sec registration times. For 700 ms inter and 10 ms inner delays our solution achieve 6.05 sec, current practice achieve 12 sec registration time. For the first case our solution provides 1.84 times faster for the second case it provides 1.98 times faster registration. As we described before, when inner communication delay becomes negligible, our solution start to achieve exactly 2 times faster registration time.

5.4.1.2. Effect of Hardware choice. Figures from 5.23 to 5.24 represent overall registration time performance of current practice of Mobile IP under different hardware settings. At Figure 5.23 we show the results corresponding to different FA hardware. At Figure 5.24 we show the results corresponding to different AAA server (HA, HAAA, FAAA) hardware.

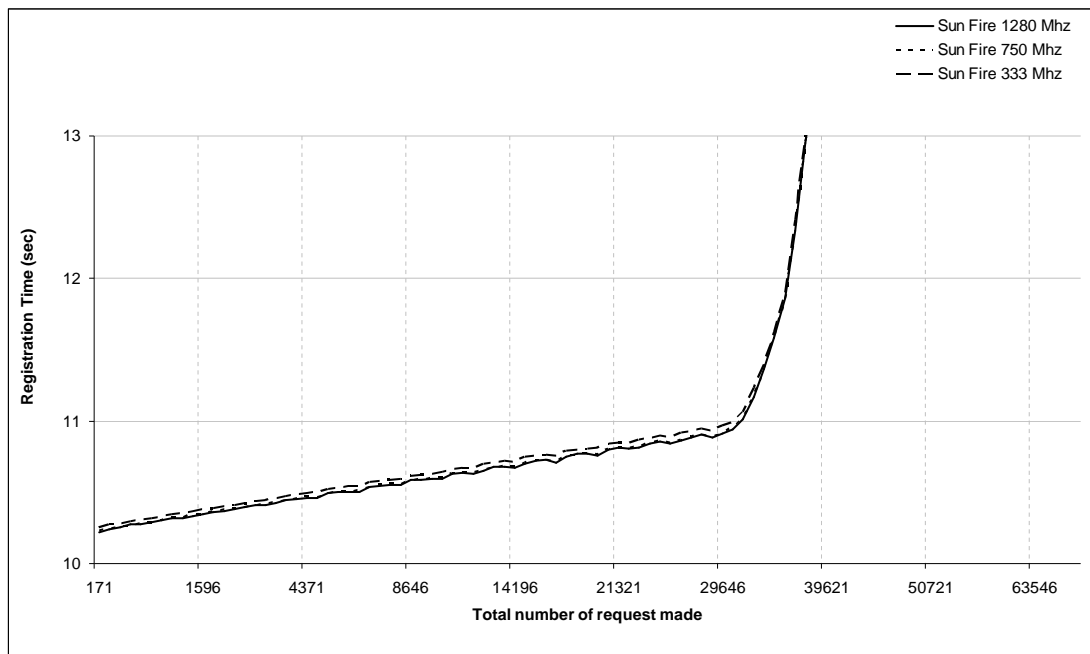


Figure 5.23. Performance of the current practice under various FA hardware.

From Figure 5.23 we can see that using more powerful FA does not improve the registration performance. Because computational workload on FAs will be low, a better hardware does not improve the results.

Using different server hardware does not alter the overall registration time till saturation occurs. Because the computational workload of a Mobile IP job is low related to the link delay affect, the performance increase at the speed of job processing become negligible.

In Figure 5.25 we show performance measure of our solution under various FA hardware. In Figure 5.26 we present same analysis under different AAA server hardware.

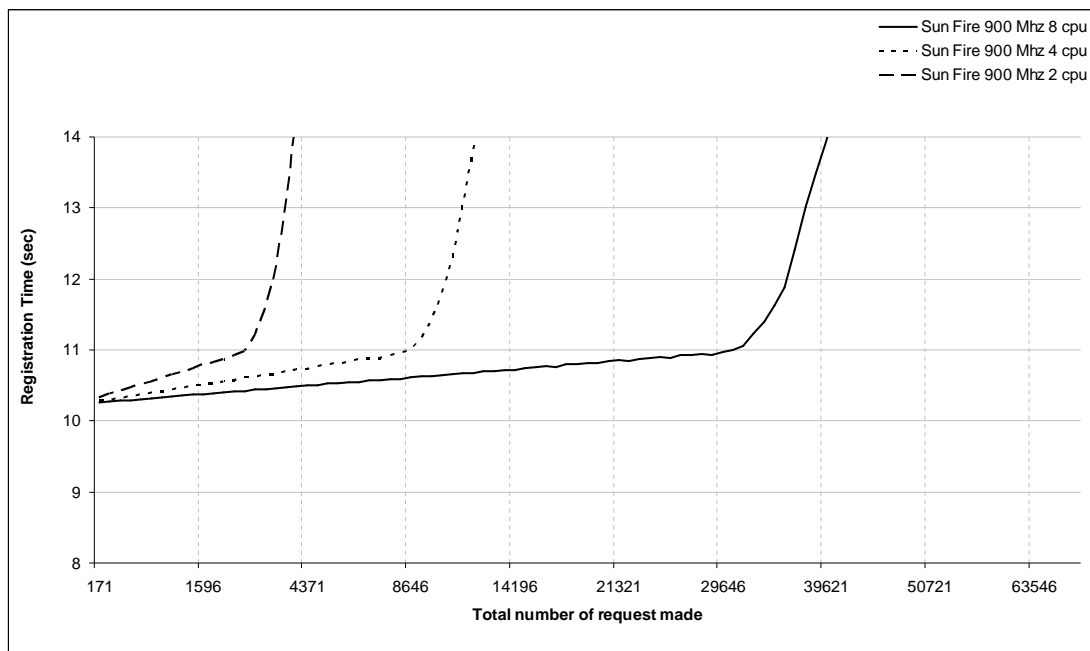


Figure 5.24. Performance of the current practice under various AAA server hardware.

When compared with current practice performance under different FA hardware, we see that our solution displays same increase pattern. Although our solution is still nearly two times faster than current practice, this property comes from link speed affect that we point out in previous subsection.

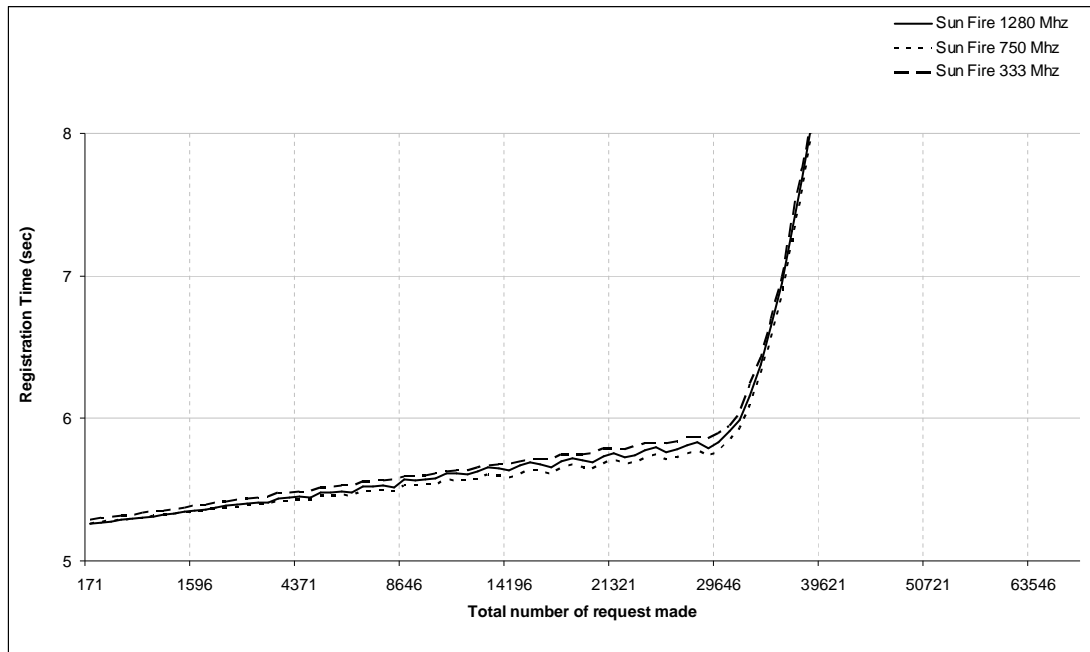


Figure 5.25. Performance of the proposed solution under various FA hardware.

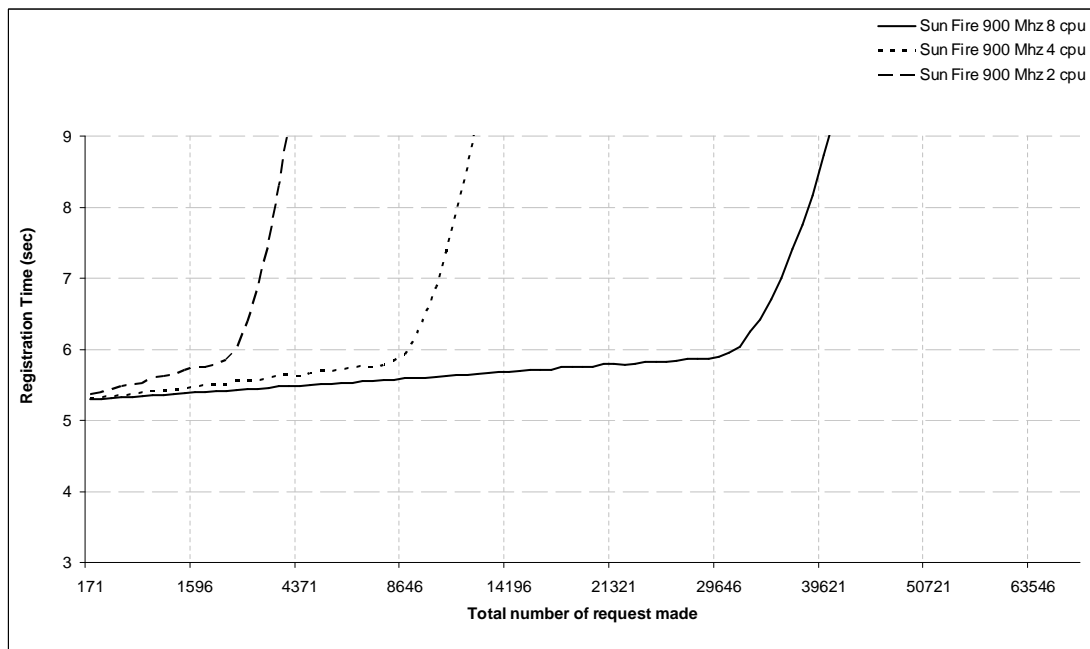


Figure 5.26. Performance of the proposed solution under various AAA server hardware.

We also see same increase pattern when we compare current performance measure from Figure 5.24 and new performance measure from Figure 5.26. At different AAA server hardware we still have a two times faster solution because of parallel link delay exerted to our communication.

5.4.1.3. Effect of Network Node Background Utilization. As in the case of different hardware settings, when we apply various background utilization to both approaches we see same increase pattern. As we explained above, due to ignorable performance loss or gain at overall processing of Mobile IP jobs we cannot detect a dramatic effect of computational power. Our solutions performance gain over link delays suppresses the computational performance gain that we achieve at different hardware settings. We think that overall affect on a Mobile IP run will not be high in real deployments too. Because of that we do not try to decrease link delays and show the affect of background utilization.

On the other hand, affect of a hardware setting becomes more dramatic when we consider system scalability. At next subsection we will further start to compare scalability of both approaches.

5.4.2. Scalability Results of Both Approaches

5.4.2.1. Effect of Link Delays. When we compare all link delay figures from Figure 5.9 to Figure 5.22 we see that all graphs tend to increase rapidly near a point of 30.000 (30.000.000 when rescaled) total number of request. This is the point where saturations on system start and scaling performance become clearer.

We can see that all link delay figures are representing same scaling performance and delays have no affect on the system performance under scaling perspective. In other words we can say scalability of Mobile IP is independent of link delays.

5.4.2.2. Effect of Hardware choice. When we compare different hardware performances of both approaches through Figure 5.23 to Figure 5.26 we can notice that FA performances do not have a critical role on scalability. We can quickly imagine that, like we did in our simulations, with steady increase at Mobile IP request made in a second, at one point FAs

also will be a bottle neck. This ignorable performance of FAs comes from fact that FAs are saturated after AAA servers. So bottleneck of overall system will be AAA servers, especially HAAA.

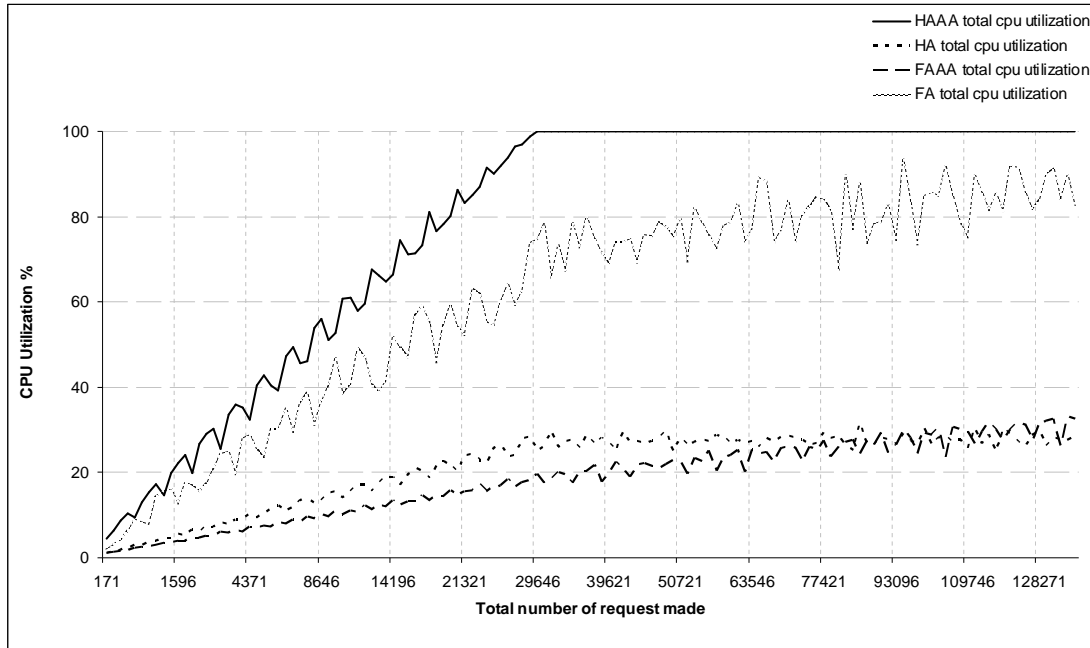


Figure 5.27. CPU utilizations of network nodes in the current practice.

From Figure 5.27 and Figure 5.28 we can see the behavior we explained. These are CPU utilizations measurements from 333 MHz FA, 900 MHz 8 CPU servers, 30 ms inner, 500 ms inter delay setup. The HAAA is saturating at near 30,000 (30,000,000 when rescaled) total number of request. This is the same point where link delay measurements have rapid increases. As we can observe from figures the other network nodes are not saturating or saturating after HAAA. So HAAA is the main bottle neck of our system so scaling performance will be highly dependent on its saturation.

Behavior in Figure 5.26 and 5.24 can be explained through this idea. When server computational capacity halved, the saturation point came at earlier total request number.

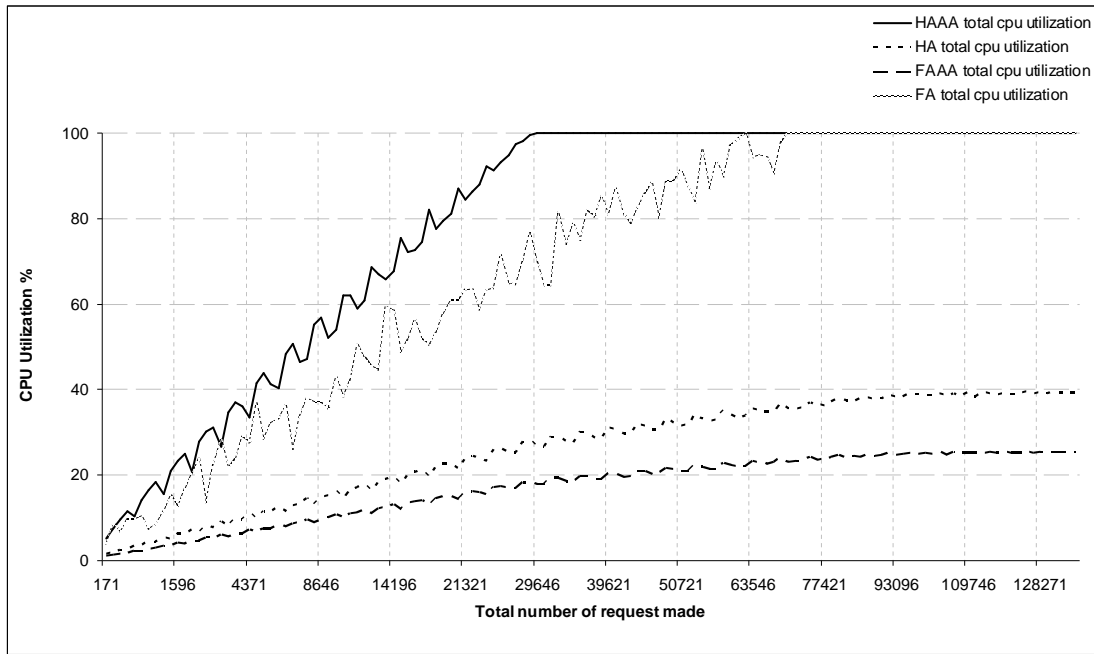


Figure 5.28. CPU utilizations of network nodes in the proposed solution.

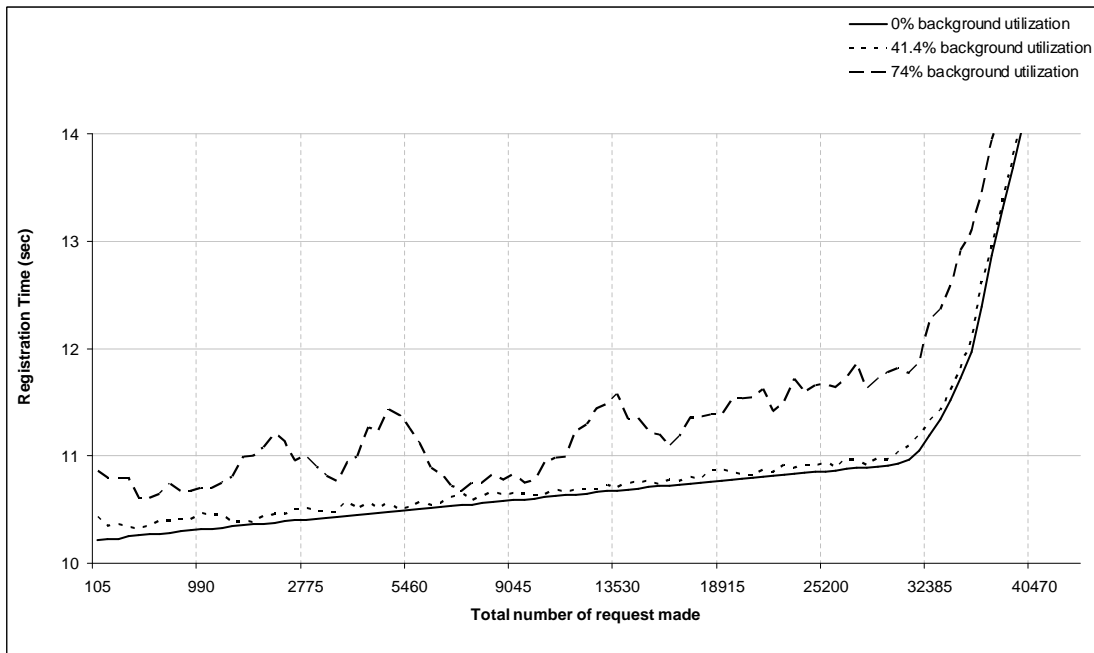


Figure 5.29. Effect of FA background utilization to performance of the current practice.

5.4.2.3. Effect of Network Node Background Utilization. Background utilization in a FA has a minor registration time affect. As we can see at most 1 sec of fluctuations can be seen when background utilization is high. But overall registration time increase pattern and scalability performance of both approaches are nearly same. There is a small amount of improvement that our solution provides. For example when we overlay Figure 5.29 and Figure 5.30 we can see that when current practice reaches nearly 40.000 (40.000.000 when rescaled) total number of request, our solution is roughly at 38.000. After rescale we see that there is 2 million total number of request difference. Although it sounds a good improvement when compare to current value, $2/40*100$, we found the improvement to be 5% only.

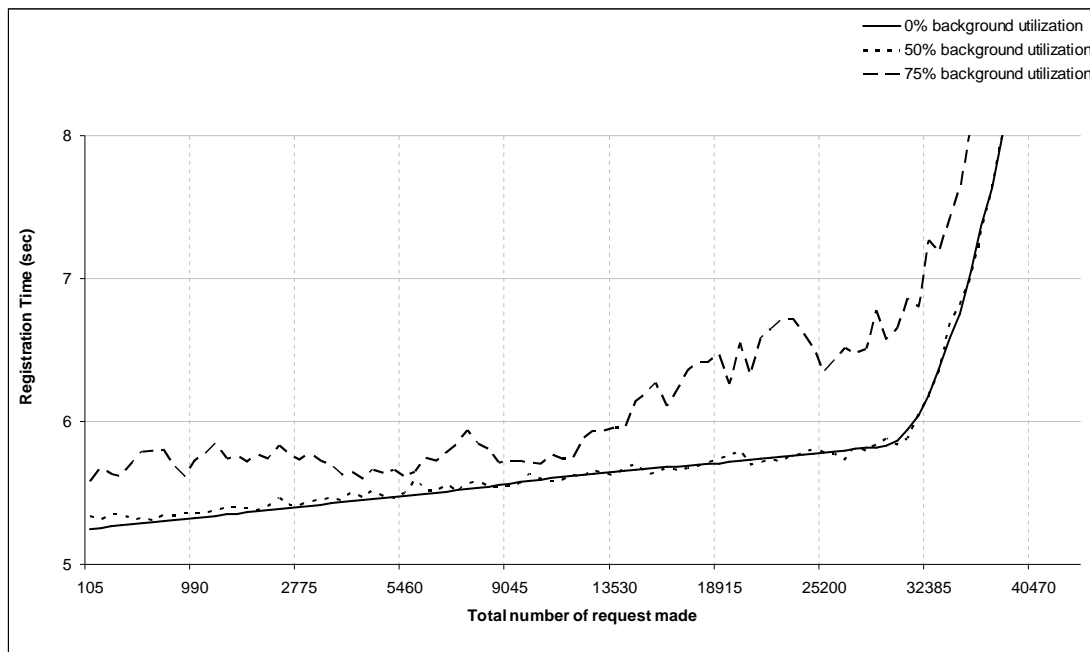


Figure 5.30. Effect of FA background utilization to performances of the proposed solution.

Background utilization at AAA servers had an observable affect as we expected. From Figures 5.31 and 5.32 we can see the decrease in scalability and registration time performance of both approaches. For example, let's look at Figure 5.31 where three settings hit 20 ms registration time; 0% background utilization setting is at 47586, 50% background utilization setting is at 27996, 75% background utilization setting is at 23220

total number of request made. We can calculate scalability performance loss with following equation:

$$\text{Loss} = (0\% \text{ performance} - \text{examined performance}) / 0\% \text{ performance} * 100 \quad (5.5)$$

With this equation we found performance loss of 50% background utilization to be 41.17%, 75% background utilization to be 51.2% for current practice. This present an interesting finding that shows using more utilized server will not perform as bad as it is utilized. When we increase utilization 50% from 50 to 75, overall performance loss increase only %24 from 41 to 51.

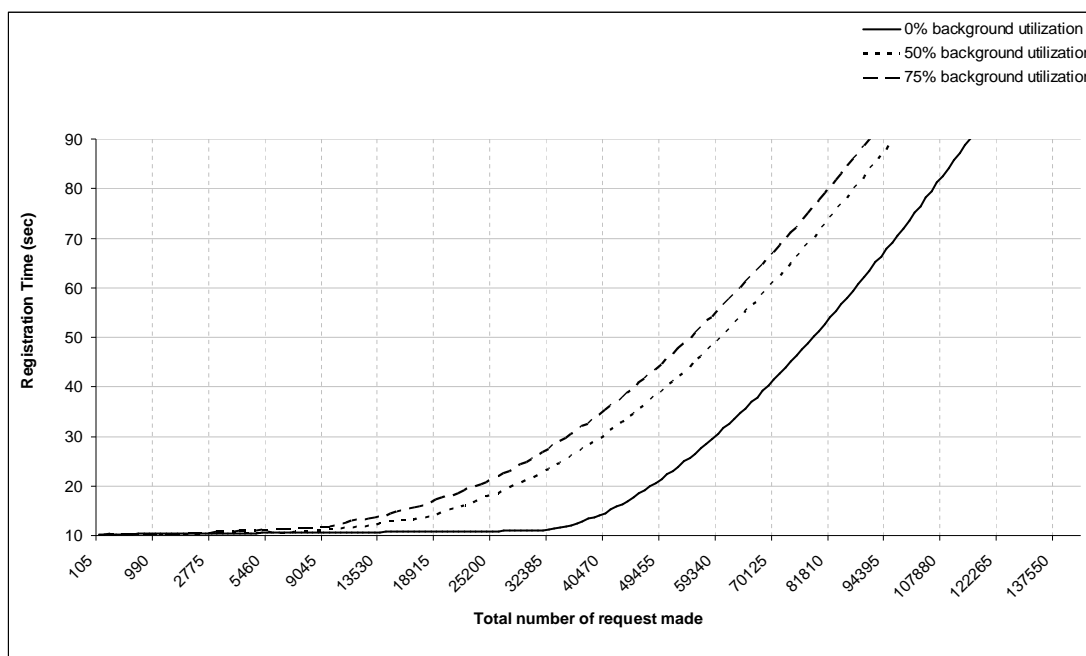


Figure 5.31. Effect of AAA server background utilization to performances of the current practice.

When we investigate our solution performance over utilized servers we observe even closer performance values for 50% and 75% background utilized servers. Three settings, 0%-50%-75% background utilization, reach 15 sec registration point at 49455, 32385, and 29403 respectively. When we compute performance we find that 50% background utilization server cause 34.5%, 75% background utilization server cause

40.5% performance loss. So when we had increased utilization 50% from 50 to 75, performance loss increase only 17.3% from 34.5 to 40.5.

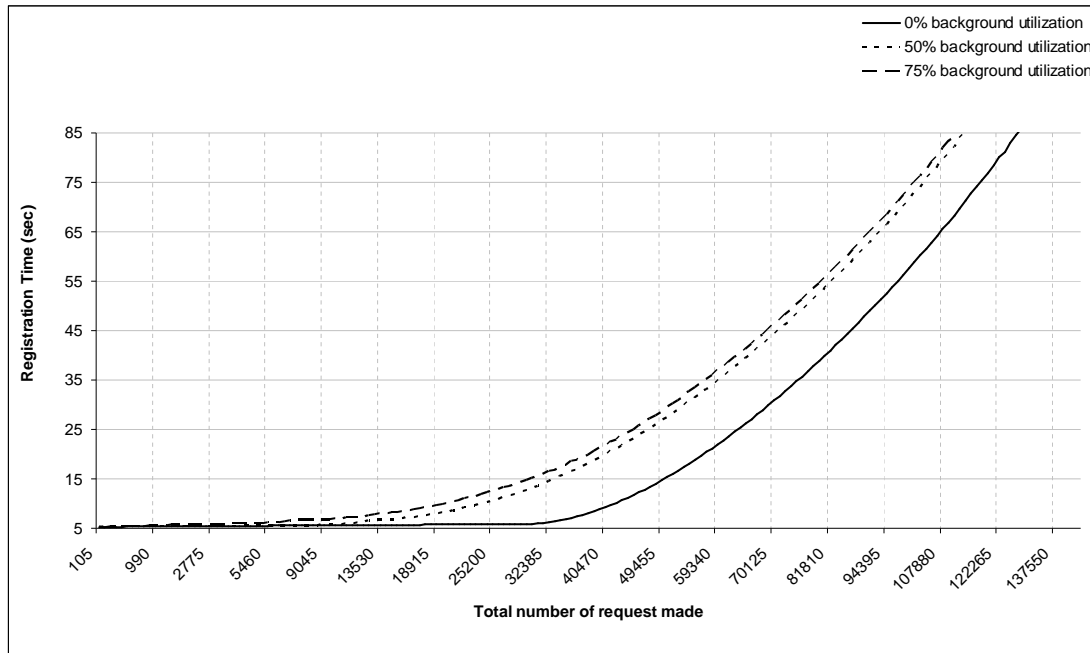


Figure 5.32. Effect of AAA server background utilization to performances of the proposed solution.

When we compare scale pattern of both approaches with background utilization settings with non-utilized server settings, we can see that when system runs on some background utilization our solution scaling performance is better than current approach. Figure 5.33 shows overlaid performance graphs of 75% background utilization setting with non-utilized server settings of both approach. But because of link delay performance benefit our solution starts at near 5 sec, current approach start at near 10 sec registration time. To see the scaling pattern clearer we shift all current approaches values with an amount calculated through comparing initial settings. By this calibration, the initial values of both approaches overlaid and scaling pattern become more obvious in Figure 5.34.

As we can see in Figure 5.34 that when there is no background utilization scaling patterns of both approaches moves more closely. But when a high background utilization is

submitted, our solution draw a wider graph which means Mobile IP requests are tolerated better after the saturation point.

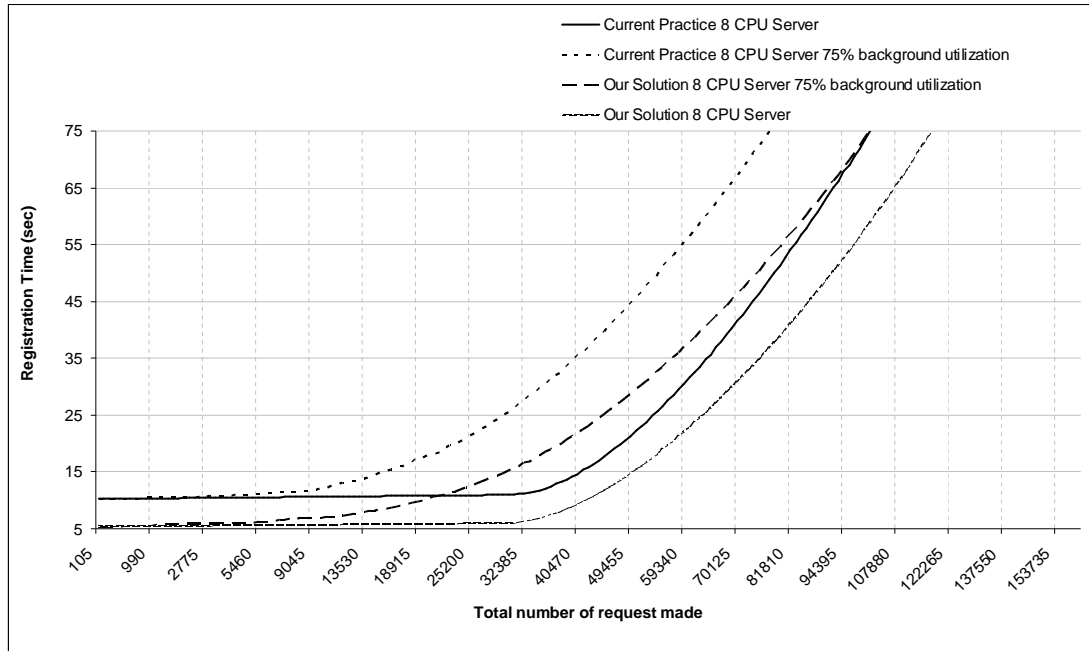


Figure 5.33. Performance of AAA servers under 75% background utilization. Overlaid performance graph.

We can look closer to the point of saturation at Figure 5.34 in Figure 5.35. We can see that when system saturated near 9453 registration request, there is a distinctive performance pattern between two approaches. When we look at non-utilized server setting there is a merely different performance graphs between two approaches.

5.4.2.4. Background Utilization versus Dedicated Computational Power. In previous subsections we showed that Mobile IP, especially with our approach, can perform well at servers which have high background utilization. In this subchapter we will try to analyze the performance difference of dedicated or shared server structures.

While creating the simulation set of hardware dependency end background utilization tests we choose special hardware and utilization numbers. For example, we used 333 MHz, 750 MHz, and 1280 MHz FA in hardware tests and 41.4%, 74% background

utilization in 1280 MHz FA for background utilization tests. With a simple math, the free computational power in background utilization tests can be calculated as $1280 \text{ MHz} * (100-41.4)/100 = 750 \text{ MHz}$ and $1280 \text{ MHz} * (100-74)/100 = 332.8 \text{ MHz}$. So with these settings we both measured dedicated performance of a server to Mobile IP and performance of a shared server which has free computational power which is equal to previous dedicated server. The idea behind this is to compare the business model to use a dedicated server for Mobile IP or share server of another applications that has enough free resource. Especially for RADIUS case, probably the ISP that will deploy Mobile IP will have some RADIUS servers already. So they may choose to run Mobile IP with same servers or expand server structure to dedicate a server to Mobile IP deployment.

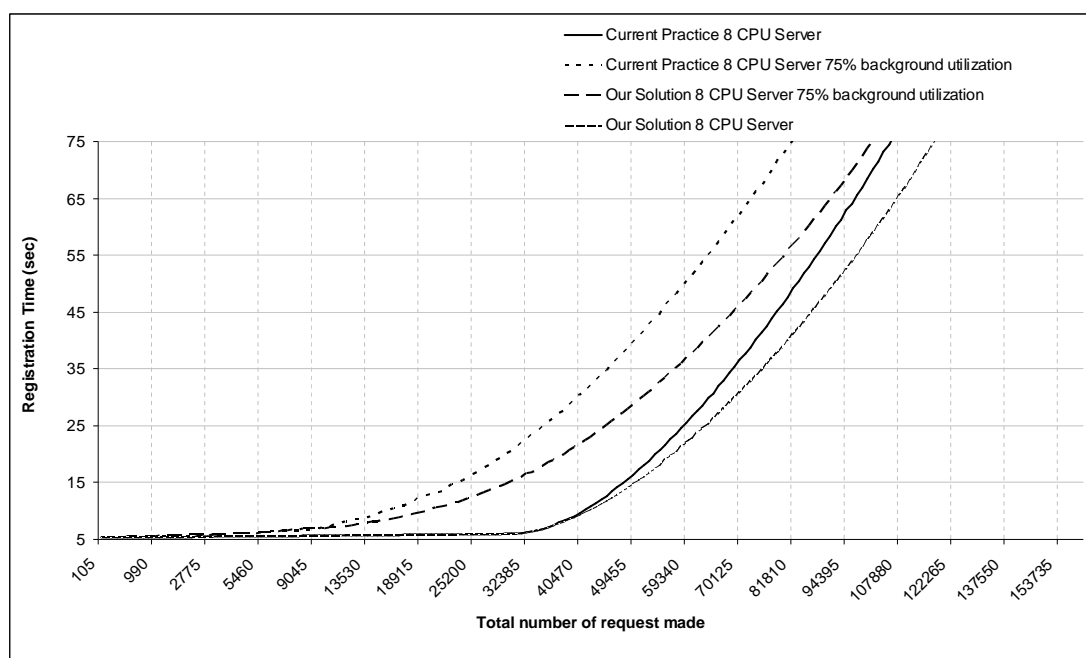


Figure 5.34. Calibration of current practice to overlay result graphs.

When we compare FA performance in Figure 5.36 we see that all 1280 MHz, 333 MHz and 74% utilized 1280 MHz server configuration behaves very closely. As we explained previously, we see this kind of a pattern because there is no saturation occurring in FA. So having a more powerful or more utilized FA does not have a dramatic effect to registration time or scalability performance of the system.

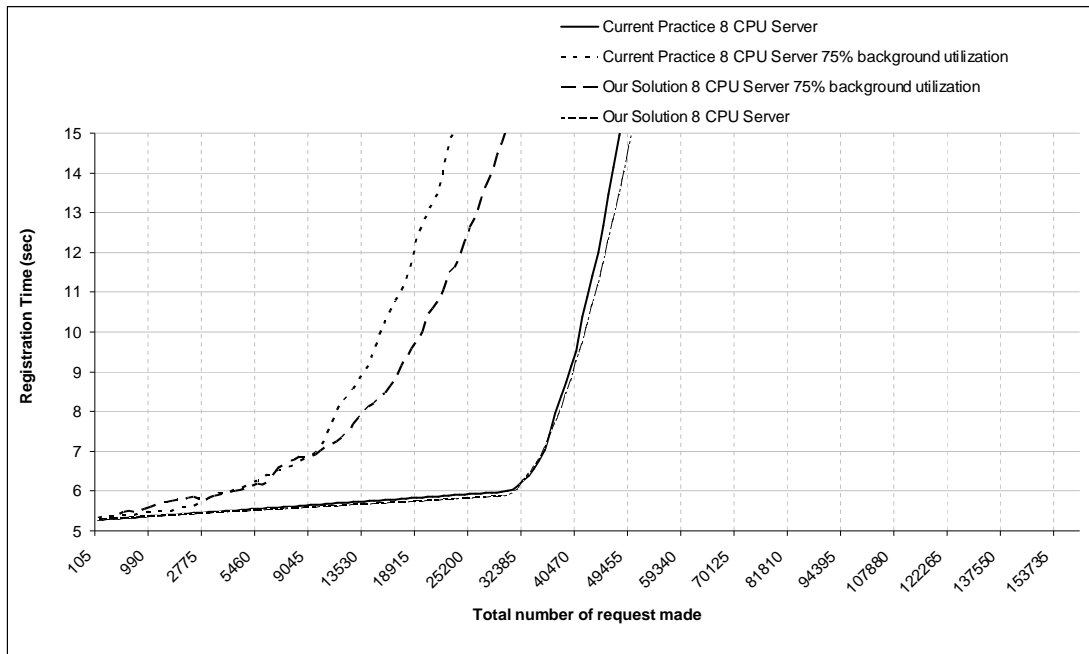


Figure 5.35. Calibration of current practice to overlay to overlay result graphs. Closer look to saturation point.

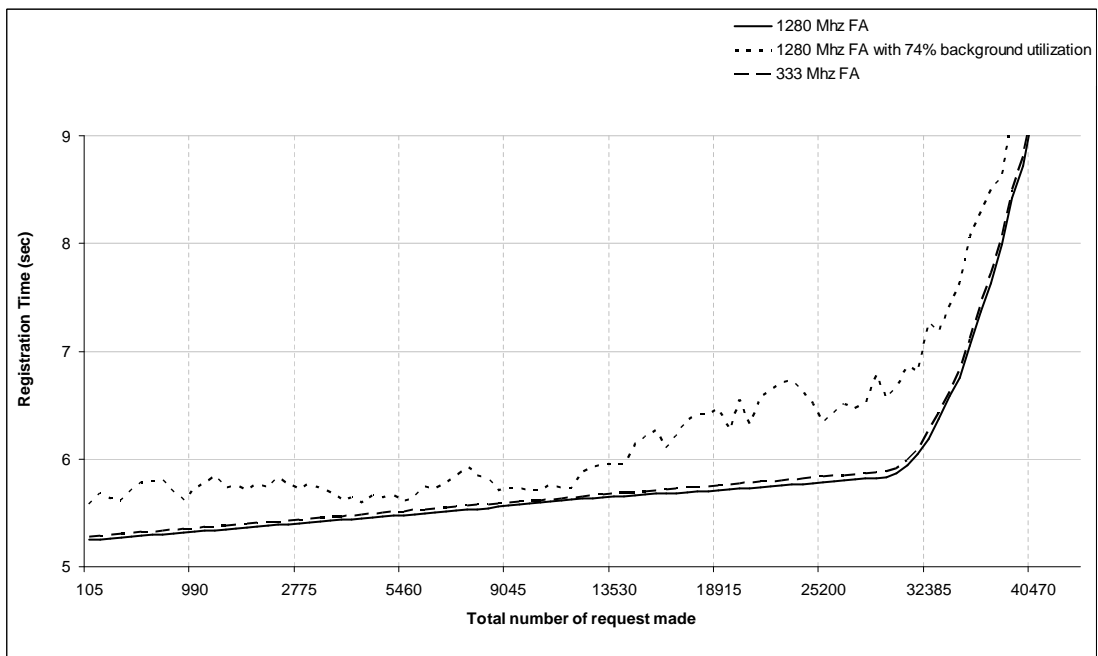


Figure 5.36. Effect of FA background utilization compared with slower hardware choice.

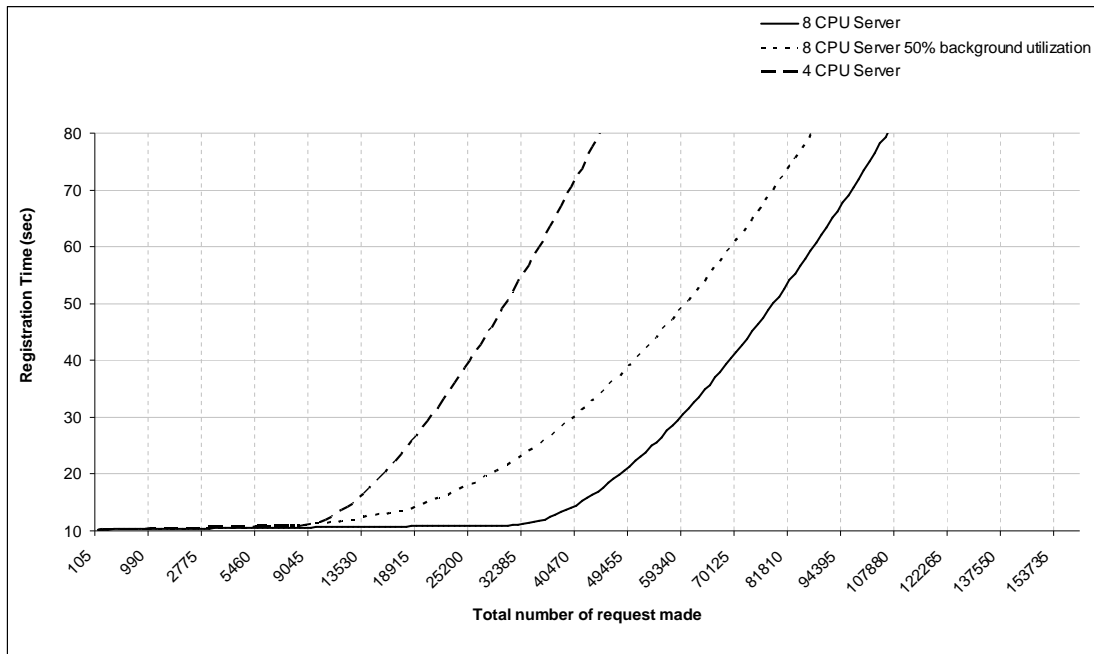


Figure 5.37. Effect of 50% AAA server background utilization to performances of the current practice, compared with slower AAA hardware choice

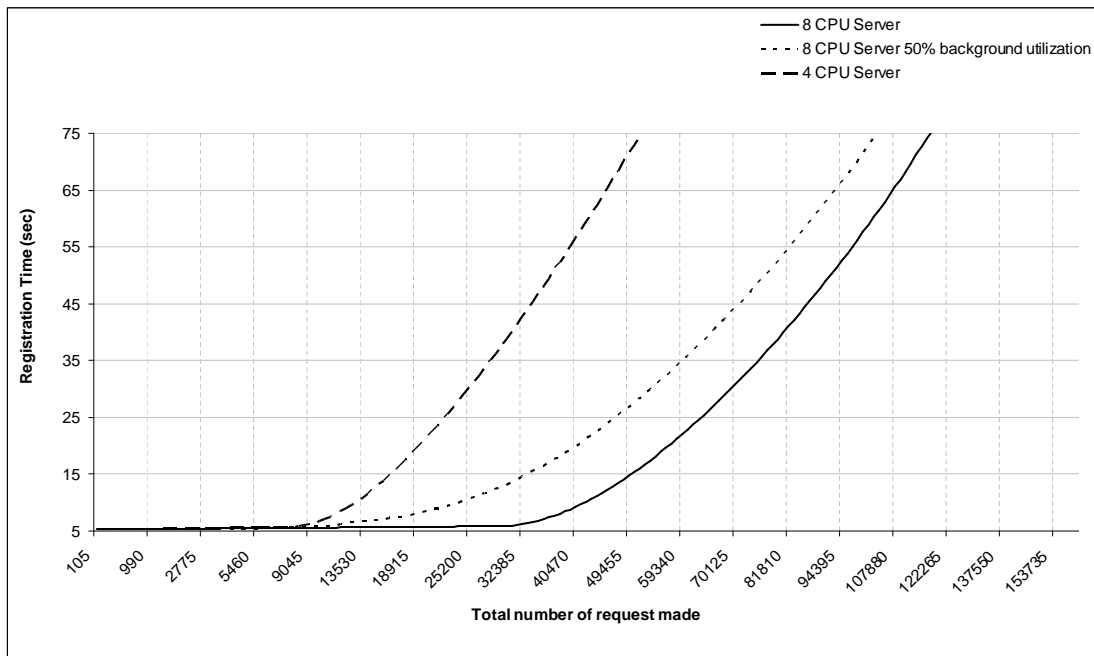


Figure 5.38. Effect of 50% AAA server background utilization to performances of the our solution, compared with slower AAA hardware choice

On the other hand, comparing server settings gives some interesting results. We can see from Figure 5.37 to 5.40 that in both approaches and both utilization level a shared server is performing well better than the dedicated server configuration.

For example let's examine the total number of request made when registration time reaches 25 sec in Figure 5.38. 4 CPU, 50% background utilized 8 CPU, 8 CPU server gives 21945, 46665, 62481 total number of request made respectively. When we calculate scalability performance loss we can find that if 4 CPU used instead of 8 CPU setting there will be 64.9% loss. If 8 CPU 50% background utilization used instead of 8 CPU setting there will be 25.3% loss.

On the other hand, in Figure 5.40, 75% background utilize 8 CPU server gives 43956 and 2 CPU server setting gives 8646 total number of request made. If 2 CPU used instead of 8 CPU setting there will be 86.1% loss. If 8 CPU 75% background utilization used instead of 8 CPU setting there will be 29.6% loss.

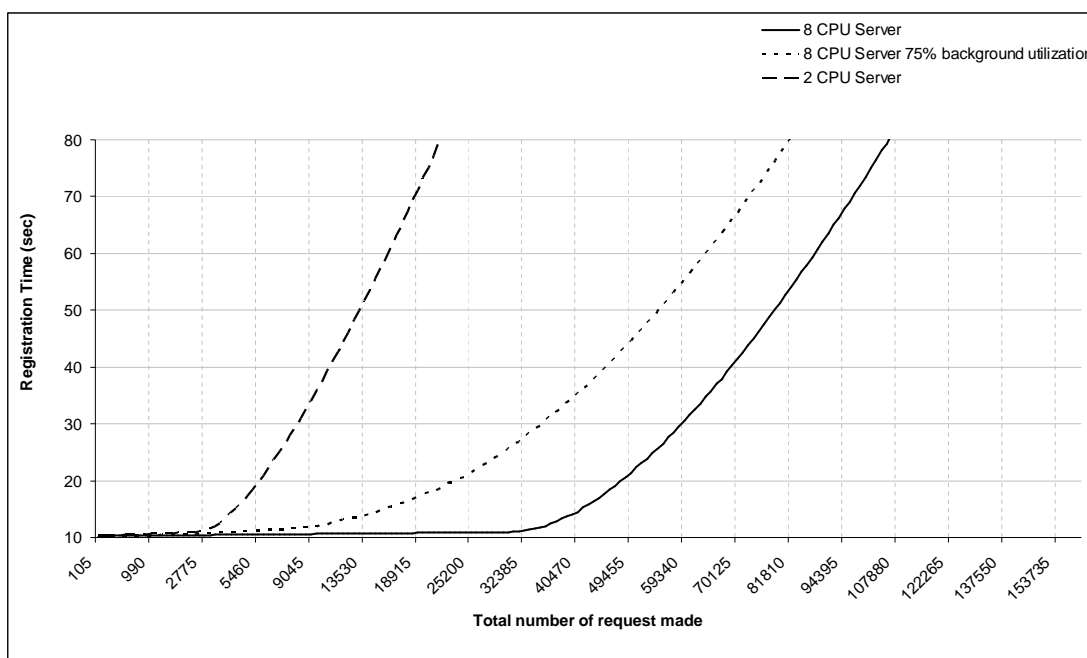


Figure 5.39. Effect of 75% AAA server background utilization to performances of the current practice, compared with slower AAA hardware choice

We can see that in all cases, background utilized (shared) servers out performs the non-utilized (dedicated) counter parts. The performance difference become dramatic when we choose more background utilization and corresponding dedicated weak hardware. For the %50 utilization case total number of request made was twice much of dedicated one. For the 75% case it is nearly 5 times more.

We can conclude that for better registration time and scalability performance a shared powerful server is the right choice even it there will be some high background utilizations.

5.5. Discussion of Simulation Results

In this subchapter, by using cell residence time from an empirical work, we provide a methodology to find active number of Mobile Nodes from number of registration request made. Moreover, we discuss expected link speeds in near future and provide a simulation result under very low link speeds. In last section of this chapter, we discuss server dedication for Mobile IP networks and argue our findings.

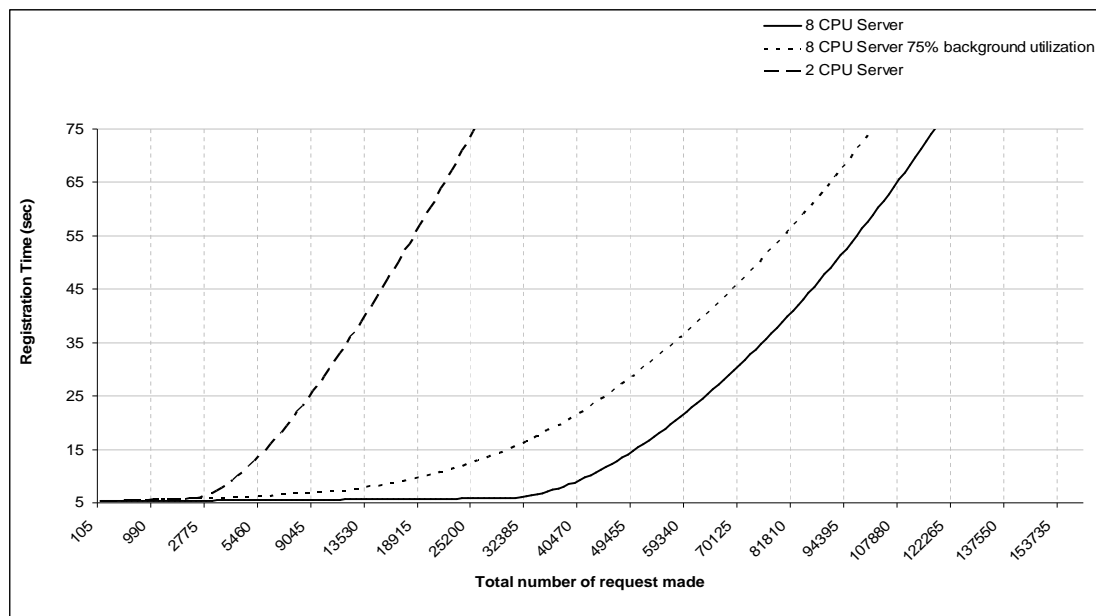


Figure 5.40. Effect of 75% AAA server background utilization to performances of the proposed solution, compared with slower AAA hardware choice

5.5.1. Active Number of Mobile Nodes

In the simulation result graphs, presented formerly, the x-axis is depicted as “Total number of requests made”. In real practice, one Mobile Nodes has to register several times while it roams in different cells. Especially for scalability analysis, to figure out how many mobile nodes that our simulation network can support, mobility pattern is needed to define a roaming and registration behavior of the nodes.

We expect Mobile IP to be used in various infrastructures like GSM, WiFi, etc. Each of these infrastructures uses different cell areas. Therefore, a mobility pattern for a possible Mobile IP network must cover patterns for both short and long range radio frequency networks. Several empirical studies performed on mobility of the nodes which can be used in our discussion. We used the mobility pattern data presented in [27] where the roaming actions of 85 users are logged for 25 days. Each user had a phone that has the capability to use Bluetooth for short range radio frequency and GSM for long range radio frequency.

Table 5.3 Cell Residence Time

Points	53155 Samples
Minimum	1 Second
Maximum	66.900 Seconds (\approx 18.28 hours)
Mean	1437.06 Seconds (\approx 24 minutes)
Median	120 Seconds
Std Deviation	4806 Seconds (\approx 80 minutes)

Results of this study are presented in Table 5.3. It is found that average cell residence time for a mobile node is 24 minutes. In order to find out the number of active mobile nodes at a specific time, we have to divide the total number of registration requests to the duration of measurements which is also divided by 24 minutes.

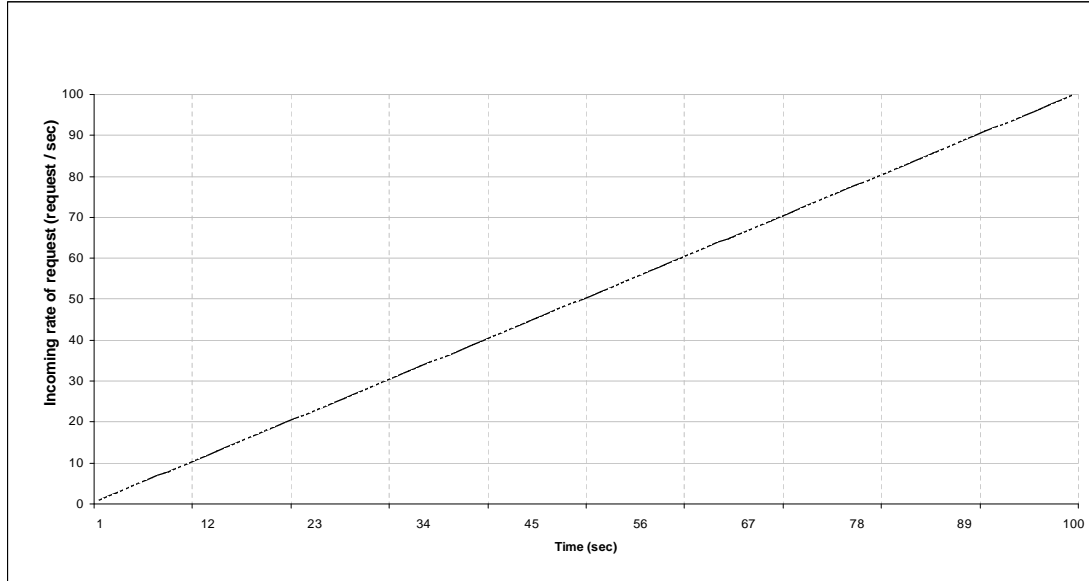


Figure 5.41. Rate of incoming request versus time.

$$\text{Number of active nodes} = \text{Total requests} / (\text{Time of measurement} / 24 * 60 \text{ sec}) \quad (5.6)$$

In our simulations, to increase the workload in time and evaluate scalability of both approach, we used increasing number of incoming registrations. The rate of increase is kept constant and defined to be dependent to time as depicted in Figure 5.41. Therefore, all the registration requests made do not enter to the system at the same time. We must find out average session time of each Mobile Node in our simulation. From Figure 5.41 we see that when the time is x , incoming number of requests is x . Total residence time of a mobile node that enters at time x , will be $t-x$ where t is time of measurement. Hence, the total time of sessions created at time x will be $(t-x)*x$. To calculate total session times from time 0 to time t , we must calculate following series:

$$\begin{aligned} \sum_{x=0}^t tx - x^2 &= \sum_{x=0}^t tx - \sum_{x=0}^t x^2 = \frac{t * t * (t+1)}{2} - \frac{t * (t+1) * (2t+1)}{6} \\ &= \frac{t^3 + t^2}{2} - \frac{2t^3 + 3t^2 + t}{6} = \frac{t^3 - t}{6} \end{aligned} \quad (5.7)$$

This formula gives the total session duration till time t . To find average session duration, we must divide this value with the total number of sessions which is $t(t+1)/2$. Then the average session duration is found to be:

$$\frac{t-1}{3} \quad (5.8)$$

Then, putting Formula 5.8 into 5.6 yields:

$$N = \frac{TR * 4320 \text{sec}}{t-1}, \quad (5.9)$$

where N is the number of mobile nodes, TR is the total number of requests and t is the time of measurement.

We can use Formula 5.4 to calculate the active mobile nodes presented in Figure 5.40. In the graph, we see that for 8 CPU non-utilized server, the point where the scalability becomes a problem, which can be called the point where system capacity is overrun, is 32,385 total number of requests which is measured at 252nd second. For 75% utilized servers, it is 2,775 requests which are measured in 72nd second. We previously explained that each computational cost scaled down 1000 time to lower the resource requirement of the simulation runs. Therefore, each result must be re-scaled before doing any further calculations. We expect 32,385,000 requests in 252,000 sec and 2,775,000 requests in 72,000 sec respectively. When we apply the Formula 5.4, we find that CPU non-utilized server's capacity is 555,171 active nodes and 75% utilized server's capacity is 166,500 active nodes. All other "total number of request" values in simulation results can also be converted to the total number of active nodes in this manner.

5.5.2. Effect of Link Delays

For the simulation experiments, we run all hardware sets under 30 ms inner, 500 ms inter link delays. In this subsection, we discuss the expected link delay patterns for the present and future deployments of Mobile IP.

We forecast that the link delays will continue to be crucial factor to determine the overall registration times. Better transmission technologies will enable slight improvements in link delays since major component of the delay is the propagation delay. Although the transmission capacities are increasing rapidly, there is not too much gap that can be filled with improvements in propagation. Propagation delay depends on the speed of light and the transmission medium. It is easy to foresee that fiber backbone infrastructure that is established all over the world will remain to be the main transmission medium for long years. Therefore, we cannot expect a decrease in propagation delays in near future.

At the time that this thesis is written, cross country land line link delays in ISP backbone networks was in range of 10 to 30 milliseconds in Turkey. This information is collected from core network engineers of the two biggest ISPs in Turkey. There is also a delay analysis that is made by Sprint Academic Research Group that validates these cross country link delay values [28]. Therefore, we expect to continue to have 20 milliseconds of cross country link delays on average in the future.

Although, we do not expect inter domain link delays to be lower than 5 milliseconds, we also run our simulations with very small link delay values. We want to show that even if the inter domain delays are close to inner domain delays, the performance difference of both approaches will be still significant. In Figure 5.42, we present the simulation results of very small link delays. As seen in the figure, with low inter domain link delays, the communication performance of both systems are found to be closer, compared to results under long inter domain link delays. But still, under 3 ms inner and 5 ms inter delay conditions, we see that our solution enables registration times to be less than 1 second for up to 9,045 total request (296,000 mobile users) where the current practice achieves similar registration time performance for maximum 5,640 requests (238,800 mobile users). Our performance is still roughly 25% better than the current practice in terms of the maximum number of mobile nodes supported under 1 sec delay.

5.5.3. Deciding Server Dedication for New Mobile IP Deployments

In this subchapter, we will outline findings on the background utilization of the servers and discuss how this information can be used for business decisions.

As shown in Figure 5.36, even if different hardware settings are used for FAs, very similar results achieved. Using a four times more powerful hardware for FAs does not produce a significant change. In the same figure, we also see that using a FA node that has 75% background utilization presents poor performance than a dedicated server that has 75% weaker server setting. Along with this information, we can argue that using a dedicated but weaker server/agent as a FA for Mobile IP communication is a better investment. This finding can be useful in decision process of investment planning for further deployment of Mobile IP hardware.

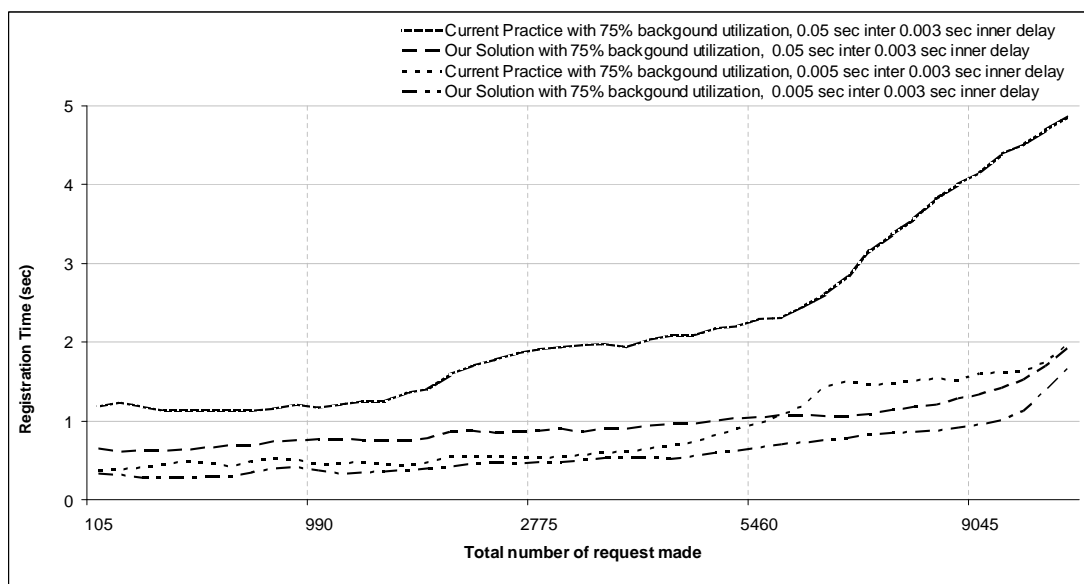


Figure 5.42. Performance comparison of the current practice and the proposed solution for very low link delays.

On the other hand, as shown in Figure 5.39 and 5.40 for the AAA servers, that using a weaker server setting has a dramatic effect on the overall performance of the system. Note that, as the figures depict, when compared to 75% weaker hardware, using

75% background utilization performs significantly better. Especially for the RADIUS servers HAAA and FAAA, it is important to realize that ISPs are currently using RADIUS servers in their production line already. When Mobile IP is deployed, ISPs must decide whether to use their current servers or deploy new ones. Our work presents that instead of dedicating a server as a Mobile IP AAA, if available, it is better to use a more powerful shared server. Since most of the ISP networks contain powerful RADIUS servers, an efficient way to deploy Mobile IP will be using these servers that are already in use as shared servers.

6. CONCLUSIONS

Mobile IPv4 is a well accepted protocol that IETF has standardized for the interoperability and mobility needs of IP networks. It enables a wireless node to move from one infrastructure to another without disrupting the TCP end-to-end communication and it is supported by most of the wireless technologies that are already being used or that are under development.

IETF draft standard “RADIUS Mobile IPv4 extensions” defines new attributes and methods to provide RADIUS support for Mobile IPv4. This standard presents the mobile node - RADIUS interactions that must occur before starting the Mobile IP registration. Since inter domain communications constitutes an important part of the registration time, the requirement of preliminary RADIUS messaging increases the overall time needed for registration significantly. By the RADIUS integration, Mobile IP nodes such as FA have to interact with Home Network more frequently which substantially increase the number of inter domain communications and therefore slows down the overall registration speed.

In this thesis, we investigate the communication overhead incurred and we propose the solution “Parallel AAA and Mobile IP” which aims to decrease the communication overhead coming along with RADIUS integration. Our proposal does not offer less messaging, rather, specifies a method of parallel transmission of inter domain communications that normally take considerable amount of time. We analytically prove that, parallel transmission of these communications presents valuable speed up on the overall registration process. It is shown that for different inter domain communication and inner domain communication durations, provided solution can perform up to 2 times faster registrations compared to the current approach.

Furthermore, we performed several simulation experiments to present the scalability patterns and the registration times of both approaches under various hardware capacity and link speed settings. In our experiments, we investigated the effect of the FA hardware in terms of CPU speed. Moreover, various AAA server hardware settings are simulated by changing the CPU speed and the number of CPUs. Another simulation study

is performed to investigate the effect of the background utilization of the servers on the performance. Various background utilization levels are defined for servers and the performance of background utilized servers are compared to the ones without any background utilization.

It is shown that for all server hardware settings investigated for FA and AAA server, the proposed protocol gives better registration time results compared to the current practice. Moreover, we find out that the hardware choice of FA or the background utilization imposed on the FA does not affect the scalability pattern and the overall registration time remarkably. On the other hand, the hardware choice of AAA servers has a significant impact on the scalability of the system since the AAA servers are the main bottlenecks of such networks. It is also shown that the background utilization on the AAA servers is a determinant factor for the overall performance. We find that a powerful 75% background utilized AAA server performs significantly better than 75% slower CPU speed and non background utilized AAA server. With this finding, we argue that when new deployments are planned, using the current AAA server infrastructure is a better business choice than dedicating weaker AAA servers. The results found can help the business decisions for future Mobile IP deployments.

We also examined the effect of inner and inter domain link delay values on the registration time. We present that for various delay settings, that includes high and low delay values, our approach outperforms the current practice for the overall registration times. In practice, distance of communication path between Home Network and Foreign Networks can vary widely. By definition, the Foreign Network and the Home Network can be in the same city, in the same country or they can be in different countries at the different part of the world. We proved that our solution performs better than the current practice for Mobile IP networks where the various Foreign Networks can be at various distance from the Home Network.

Finally, we provided a methodology to calculate the number of active Mobile Nodes from the number of registration requests and present number of Mobile Nodes for some of the results. The case where inter and inner domain communications are both very

low is also discussed and it is presented that the proposed solution still increase the registration speed.

As a future work, it is worthwhile to investigate the effect of other server operations, such as database search, server I/O and operating system cost, to performance and scalability. OPNET has many more features that can be used to provide more realistic simulation environment. Furthermore, by using this simulation environment, other studies and proposed solutions can be investigated in terms of scalability and registration speed. Moreover, the proposed solution can be compared to Mobile IP with DIAMETER which is the successor of Mobile IP with RADIUS.

REFERENCES

1. Jing, H., L. Jie and Y. Kun, "A Novel Commitment-based Authentication Protocol Based on AAA Architecture for Mobile IP Networks", *Wireless Communications and Networking Conference*, pp. 3558-3562 2007.
2. Perkins, C. E., "Mobile IP join forces with AAA", *IEEE Personal Communications*, vol. 7, issue 4, pp. 59-61, August 2000.
3. Perkins, C. E., *IP Mobility Support for IPv4*, RFC 3344, IETF, August 2002.
4. Taeyeon P. and A. Dadej, "OPNET simulation modeling and analysis of enhanced Mobile IP", *Wireless Communications and Networking*, Vol. 2, pp. 1017-1024, 2003.
5. Blondia, C., N. Van den Wijngaert, G. Willems and O. Casals, "Performance analysis of optimized smooth handoff in mobile IP", *Proceedings of the 5th ACM international workshop on Modeling analysis and simulation of wireless and mobile systems*, September 28-28, Atlanta, Georgia, USA, 2002.
6. Nakhjiri, M., K. Chowdhury, A. Lior and K. Leung, *RADIUS Mobile IPv4 extensions*, draft-nakhjiri-radius-mip4-02.txt, IETF, October 2005.
7. Glass, S., T. Hiller, S. Jacobs and C. Perkins, *Mobile IP Authentication, Authorization, and Accounting Requirements*, RFC 2977, IETF, October 2000.
8. Hess, A. and G. Schafer, "Performance Evaluation of AAA / Mobile IP Authentication", *In Proc. Of 2nd Polish-German Teletraffic Symposium*, Gdansk, Poland, September 2002.
9. Calhoun, P., T. Johansson, C. Perkins, T. Hiller, Ed. and P. McCann, *Diameter Mobile IPv4 Application*, RFC 4004, IETF, August 2005.

10. Kim, H. and H. Afifi. "Improving Mobile Authentication with New AAA protocols". In *Proc. IEEE International Conference on Communications (ICC)*, pages 497–501, May 2003.
11. Zhen, Z. and S. Srinivas, "AAA architecture for Mobile IP in Overlay Networks", *IEEE Conference on Local Computer Networks 30th Anniversary*, 2005.
12. Donghai, S. and T. Chaojing, "An authentication Method on Security Association for Mobile IP fast handoff", *Proceeding International Conference on Wireless Communications, Networking and Mobile Computing*, vol. 2, pp. 1324-1327, 2005.
13. Jacobs, S., *Mobile IP Public Key Based Authentication*, <http://tools.ietf.org/id/draft-jacobs-mobileip-pki-auth-00.txt>, August 1998.
14. Zao, J., S. Kent and J. Gahml, "A publickey based secure Mobile IP", *Wireless Networks*, vol.5 (5), pp. 373 – 390, 1999.
15. Chou, C., S. Min and W. Jian, "A Solution to Mobile IP Registration for AAA", *Proceedings of 7th CDMA International Conference*, IEEE, Seoul, 2002.
16. Wangle. and B. Yang, Timestamp based Mobile IP registration integrated with AAA. *Journal of Xidian –University*, vol. 31(6), pp. 952-954, 2004.
17. Xuefei, C., K. Weidong and L. Huaping. "Secure Mobile IP Registration Scheme with AAA from Parings to Reduce Registration Delay", *International Conference on Computational Intelligence and Security*, vol. 2, pp. 1037-1042, 2006.
18. Lee, B., D. Choi and H. Kim, "Mobile IP and WLAN with AAA authentication protocol using identity-based cryptography", *Proceedings of International Conference on Telecommunications ICT*, IEEE, New York, 2003.

19. Jeong, K. C., "ID-Based Secure Session Key Exchange Scheme to Reduce Registration Delay with AAA in Mobile IP Networks", *Lecture Notes in Computer Science*, issue 3515, pp. 510-518, Springer-Verlag, 2005.
20. Kim, G. H. and C. D. Ho. "Session Key Exchange Based on Dynamic Security Association for Mobile IP Fast Handoff", *Computational Science and Its Applications – ICCSA*, 2004.
21. Dai, W., *Speed Comparison of Popular Crypto Algorithms*, <http://www.cryptopp.com/benchmarks-amd64.html>, 2007.
22. Perkins, C. and P. Calhoun, *AAA Registration Keys for Mobile IP*, RFC 3957, IETF, March 2005.
23. Perkins, C. And P. Calhoun, *Mobile IP Challenge/Response Extensions*, draft-ietf-mip4-rfc3012bis-04, IETF, June 2005.
24. Rigney, C., W. Willats, and P. Calhoun, *RADIUS Extensions*, RFC 2869, IETF, June 2000.
25. Zorn, G., *RADIUS Attributes for Tunnel Protocol Support*, RFC 2868, IETF, June 2000.
26. Krawczyk, H., M. Bellare and R. Canetti, *HMAC: Keyed-Hashing for Message Authentication*, RFC 2104, IETF, February 1997.
27. Sricharan, M. S. and V. Vaidehi, "Mobility Patterns in Macrocellular Wireless Networks", *IEEE - ICSCN 2007*, pp. 128-132.
28. Sprint Academic Research Group, *Delay Analysis*, <https://research.sprintlabs.com/delaystat/>