

Trust Transfer Mechanism for Mobile Internet Access

Yonghui ZHANG^{1, a}, Zhangxi LIN^{2, b}, Jianhua LIU^{1, c} and Quan LIANG^{1, d}

¹ The Key Laboratory for Automotive Electronics and Electric Drive of Fujian Province,
Fujian U. of Tech, Fuzhou, 350118, China

² Dept. of ISQS, Texas Tech U. Lubbock, TX 79409-2101, USA.

^azyh@fjut.edu.cn, ^bzhangxi.lin@ttu.edu, ^cliwen@fjut.edu.cn, ^dlq@fjut.edu.cn,

Keywords: RSVP handover; trust transfer; context transfer; authentication mechanism

Abstract. Multimedia applications bring demands on broadband real-time data transfer, which needs resource reservation protocol (RSVP) helps to satisfy. However, handover processes bring delay, and existing authentication mechanism makes it further worse. Based on Pareto distribution patterns of mobile station communication traffic, proposed a trust transfer mechanism to execute pre-anticipated trust transfer and shorten the delay. It means that the dominant minority correspondent nodes designed in the VIP address books are informed about trust context messages, such as the information of handover, AAA, QoS, before anticipated handover. With the trust transfer mechanism, the simplification can be made to the authentication mechanism, which divides trust handover sequencing into several paralleled parts and budes some steps between stations. Thereby cut processes on each node by processes simultaneously carrying. Simulation with a modified NS2 platform showed that when time setforward equals 0.2, the delay is reduced by about 19.12% and the resource possession of RSVP is mitigated by 30.13%.

Introduction

High-speed mobile multi-media in portable Internet becomes multimedia applications rapidly advance in mobile Internet, with demands of broadband and real-time transfer. Only mobile IP scheme such as Hierarchical Mobile IP[1] or fast handover Mobile IPv6[2] cannot support it very well, as a consequence of challenges, such as seamless handover (HO) and the QoS (Quality-of-Service) during the HO process[3]. It must work with the resource reservation protocol (RSVP) to ensure the QoS, broadband transfer and real-time transfer.

However, though it is designed for QoS, RSVP is so difficult to execute in handover processes because MIP buffer packets and then buffer enlarges delay so QoS demands are hard to be satisfied. Moreover, packets in tunnels cannot get the same QoS. MRSVP, MIPRSVP, and Dynamic RSVP, series of RSVP protocols[4] all requests reservation resources be reallocated *before* handover (HO). Since next-cell prediction is uncertain, it can but reserve resources at all possible place, which makes high frequency of IP-in-IP tunnel, afterwards, introduces extra overhead.

Further, the current authentication mechanism makes things worse. It uses the AAA server to carry authentication security, with plenty of complexity. Diameter AAA access authentication defined by IEEE needs 18 steps to build the authentication security process[5], while Radius is up to 32 steps, is exacerbated by the delay[6], which can make resource reservation timeout in great probability, not to mention services.

We designed a mechanism for the dominant minority based on Pareto pattern on communication traffic of mobile station, then, showed more details in trust transfer mechanism. Analysis and the simulation validated the availability.

Table 1. Acronym: full name

ABI: address book informing	CoA: care of address	MN: mobile node
BU: binding update	HA: home agent	MR: mobile router
AR: access router	HO: handover	SA: security association
CN: correspondent Node	HoA: home of address	

Table 1 shows common acronyms appear in this paper.

Trust Transfer Processes

Noted that majority of communications traffic is for a limited size m of callers or callees in corresponding nodes (CN) group[7], set up the VIP address book contains m members ($m=20$ in our experiment, but can vary according to user level requirements for QoS). m denotes mobile nodes and mobile routers (MR) on which traffic concentrate, so that 95% of call traffic can be covered. So it means $\exists m, \forall P(\xi > m) \geq 95\%$. The classified aggregations of the data distributions on the communication traffic comply with Pareto distribution described as following:

$$y=B*x^{-1-a}. \quad (1)$$

Where x denotes communication times or traffic (Mb), and y denotes how many CNs at the same frequency (call/month or Mb/month). With Unicom communication data, we have extended the statistical range in [7], and have got the coefficients range as follow: $B=16\sim 22$ and $a=0.067\sim 0.087$ for subtotaled by communication times or calls; while $B=1.37\sim 1.52$ $a=0.86\sim 0.97$ for communication traffic (Mb). $R^2=0.960$, shows the data obeys Pareto distribution. This outcome is similar to the conclusion on distribution characteristics of FTP files reported.

Trust transfer was optimized for the dominant minority group of callers or callees, which defined in a special VIP address book. Aiming to improve the 95% real-time services, mobile station will keep all these CNs informed of trust context messages in advance. So the above method was called address book informing, or ABI. Trust context in ABI messages contains QoS, AAA and HO messages, such as expiration data, the current Care of Addresses (CoA) of mobile nodes (MN) and the list of possible next Access Router (AR). Trust context transfer mechanism with ABI is just a frame containing information. QoS, AAA, and HO information will be forwards to relational nodes.

When in handover, trust transfer with ABI can also make the function. The original idea of tunneling buffer packets is smooth HO, but introduces more delay and difficulty of guaranteeing QoS in tunnel. With the mobile speed of mobile node (MN) increases, two and more tunnels may be needed. Things turn worse. Now if binding update cannot be achieved in time, previous access router (PAR) originally forwards packets from its corresponding CNs to the home agent, but now it is PAR can send the packets to next AR (NAR), which does not take a detour and then makes high-frequent IP-in-IP tunnel.

To avoid RSVP in tunnel, some literatures adopted the similar method, for example, Chaudet introduced mobility notification and location register[8], Yet cannot solve the call initialization question. Of course, MN have informed each of its CN of its CoA, but most of them achieve the optimized routing only *when* MN initializing a call or *after* CN initializing a call. However, if it is *when* CNs initialize a call, since CNs cannot know the CoA of MN and still have to go through HA of MN, there still forms a similar triangle routing. It prolongs waiting time of initializing. The phenomenon exists in almost all mobility schemes, no matter in HMIPv6, FastMIPv6, or the HADL scheme based on dual-link. The higher mobility speed of MN is, the worse the problem becomes, because the frequency of third party HO is increasing, the more cooperation steps between MN and ARs must be finished.

In the call initializing process with ABI, once a MN receives all these CNs context messages informed, it can prepare for the HO and be ready to rebuild an RSVP QoS path. Since MN and the current AR have known the next AR, most IP-in-IP tunnels can be avoided lest RSVP expires on preparing period. Therefore routing, HO and QoS got further optimized, which speed up the initialing process and partly solves the delay in the HO process. It is by multicast or by unicast that AAA, QoS and HO context can be sent to MN's probable next cell. By multicast is a better method. If only the contexts can be transferred before HO, the HO delay will be shortened and MSPEC can be minimized.

Time Sequence of Simplifying Authentication Mechanism

Our Trust Transfer Mechanism bases on ABI method, and can make a novel trigger time sequences as showed in Fig 1.

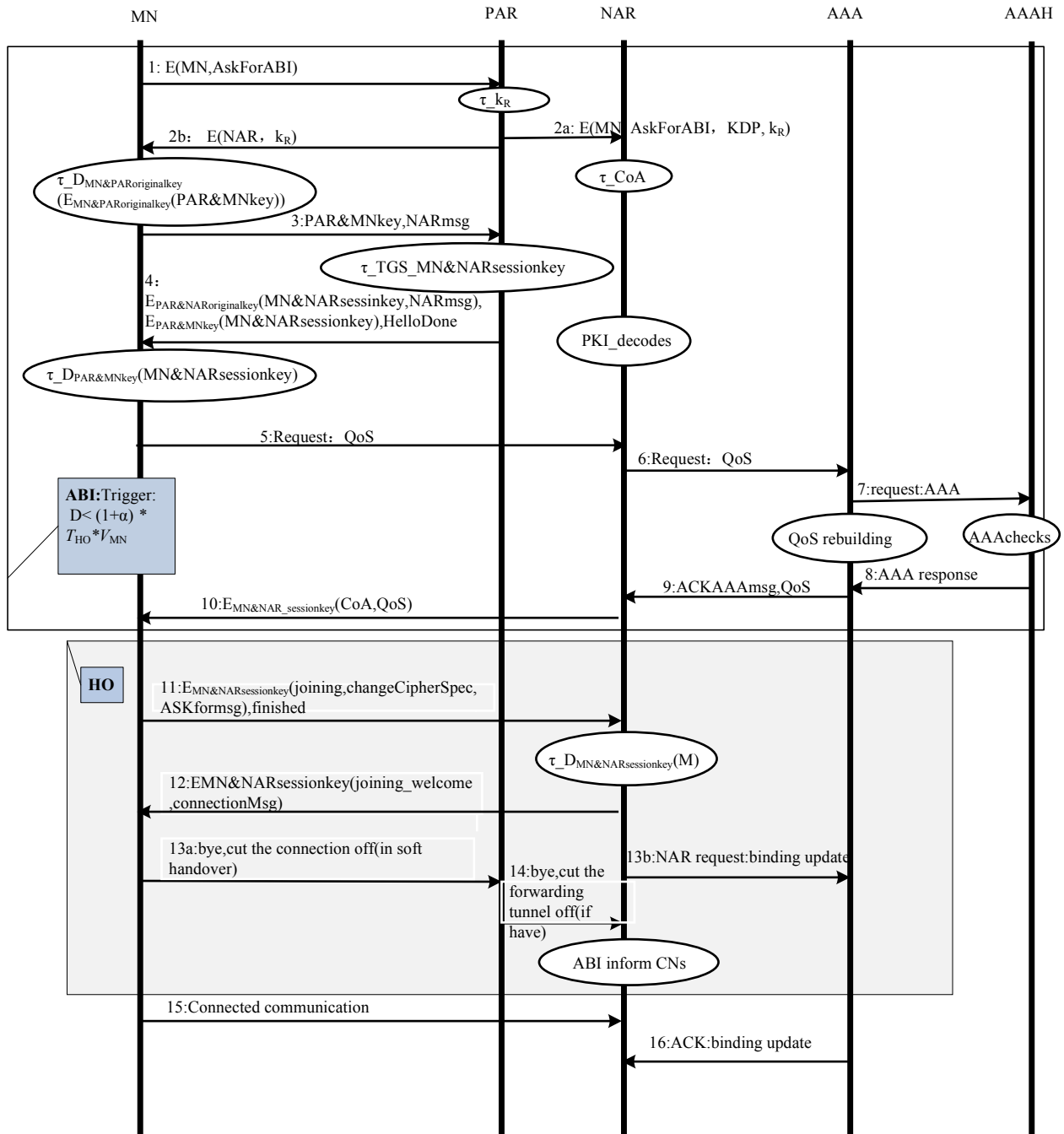


Figure 1. Time Sequence of Trust Transfer Mechanism

Trust transfer context information can help to simplify the AAA process. There are 10 steps processes before HO, and six steps processes in HO step, which means greatly reducing in the AAA steps.

When a MN is approaching the rim of the edging of a cell, the trigger mechanism of trust transfer mechanism will be triggered preparing for HO. The edging cells denote the access router (AR) that the cell belongs to have a boundary with another router. Only the edging cells of a router need considering IP layer HO. Trigger distance D_{trigger} from rim of the edging cell can be calculated by

$$D_{\text{trigger}} = (1 + \alpha) T_{\text{HO}} V_{\text{MN}}. \quad (2)$$

Where α is the time setforward, $\alpha=1$ means double of the HO time, while $\alpha=-1$ means no time setforward. α is an empiric value decided by experiments in order to insure the trigger mechanism, so that α greatly affects the quality of HO; T_{HO} is HO time; V_{MN} , the velocity of MN, can be acquired by wireless positioning with GPS info or sensor network and E-map.

The time sequence of simplifying authentication mechanism is shown as following.

- 1) Once triggered, MN asks PAR for ABI, with the message E (M).
- 2a) PAR forwards the message to the NAR with a random key k_R .
- 2b) at the same time, PAR replies to k_R MN.
- 3) MN affirms the new key.
- 4) PAR replies the session key and finishes the key distribution.
- 5) MN rebuilds the QoS path in the NAR.
- 6) NAR verifies the QoS agreement in the local AAA server.
- 7) Local AAA asks the foreign AAA server for the verification.
- 8) AAAF makes response.
- 9) AAA makes responses.
- 10) NAR affirms the QoS and CoA information.

Now the ABI process ends and the HO processes begin.

- 11) MN asks NAR for connection with the encode key k_R .
- 12) NAR show the welcome message.
- 13) MN cut the connection with NAR.
- 14) PAR cut the forwarding tunnel off (if exists).
- 15) MN connects with NAR.
- 16) Binding update has been finished.

So the HO authentication processes can be shortened to six steps for the dividing handover sequencing into several paralleled parts and budges some steps between stations. Thereby cut processes on each node.

Simulation

Simulation is conducted to verify availability of the above framework with modified NS2 platform. NS2, replacing network simulator version 2, can be found at <http://www.isi.edu/nsnam/ns/>.

The platform was composed of 256 50km-diameter cells C_i ($i=0-255$). It is assumed that there are j MS $_j$ ($j=0-9999$) and their initial location ($C_{j0}=C_i$) and their constant speed (v_j) is randomly generated, with speed v_j from 1km/h to 120km/h. The next location (C_j^1), which decides movement direction, is randomly generated per seconds. Initiation of a call between two MS is also randomly generated on when (t_p), who (MS $_{p1}$) to who (MS $_{p2}$), how long (conversation time t_p , obeys negative exponent distribution, average value $1/\mu=200s$) and how large (bandwidth requirement B_p).

Table 2. The effects of time setforward α

α	-1	-0.8	-0.6	-0.4	-0.2	0	0.2	0.4	0.6	0.8	1
average(MSPEC)	1	1.031	1.094	1.175	1.258	1.388	1.569	2.126	3.105	3.862	5.095
ABI-HO delay(s)	2.474	2.036	1.822	1.693	1.603	1.568	1.476	1.467	1.463	1.459	1.458
resource engross(%)	10.71	11.85	12.12	12.51	12.70	12.91	13.77	15.86	18.35	26.12	37.04

With time setforward α increases from -1 (means no any time setforward, it is a common Fast HO scheme) to 1, the HO delay is reduced. When α valued -1 to 0 the delay decreases evenly and the resource engross increases evenly. From α valued from 0 to 1, the delay not obviously increases, but the resource bandwidth engross augment greatly therefore useable bandwidth is greatly reduced. One maybe explanation is that with the setforward increase, system got enough time to prepare, but the next-AR-predict become vaguer, so an aggregate of locations augment, then MSPEC of resource reservation is more. With α increases (from -1 to 1, step 0.2), average MSPEC number increases too. There exists the best compromise result in $\alpha=0.2$, with acceptable resource engross and a little HO delay.

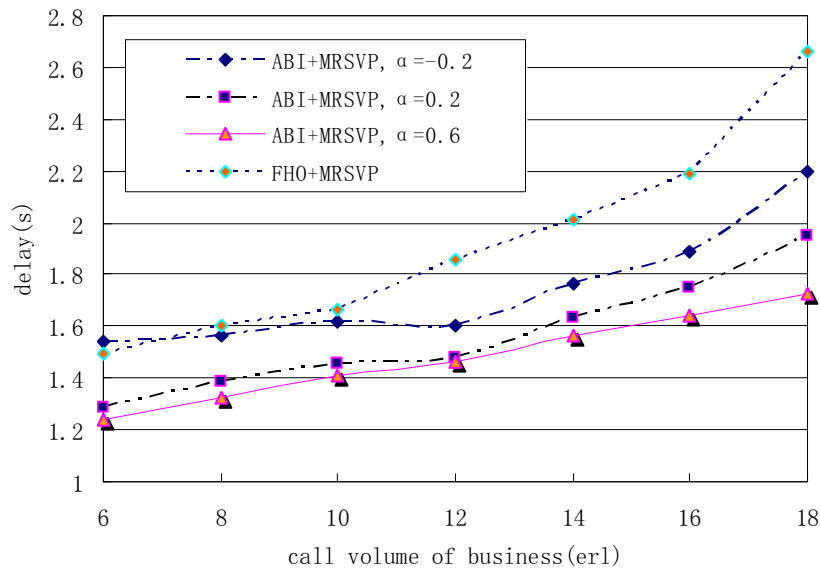


Figure 2. The effect of time setforward α on delay

Fig.2 show that the effect of time setforward α on the average of the delays in Fast HO+MRSVP[9](called FHO+RSVP) and our scheme (ABI+MRSVP) when $\alpha = -0.2, 0.2, 0.6$ and call volume of business (erl) shifts from 6 to 18.

Obviously, delays in ABI+MRSVP are smaller than FHO+RSVP no matter α is $-0.2, 0.2$ or 0.6 . Since best result exists $\alpha = 0.2$ from Table 2, the ABI+MRSVP average delays when $\alpha = 0.2$ is adopted to compare with FHO+RSVP, we have the reduced quantity of 19.12%.

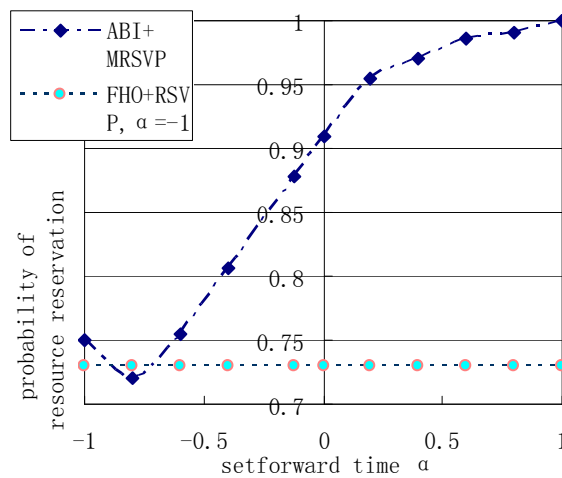


Figure 3. The effect of α on the average probability of resource reservation

Fig.3 show that the effect of α on average successful probability of resource reservation. When $\alpha = -1$, no time setforward thereby no overhead. When $\alpha = -0.8$, ABI+MRSVP performs worse than FHO+RSVP due to time setforward get too rare to prepare the ABI, much less the simplifying authentication mechanism. Howbeit ABI signaling overhead exists, so resource reservation possibilities are a little small than the FHO+RSVP. Only when $\alpha > -0.6$, the scheme is meaningful. When $\alpha = 0.2$, we can see, a large resource reservation probability with little overhead can be gotten. In the situation, and the resource possession of RSVP is mitigated by 30.13% comparing with FHO+RSVP.

Summary

This paper proposed the trust transfer mechanism for mobile Internet access with ABI scheme. With pre-anticipated trust transfer for dominant minority correspondent nodes and the time sequence of simplifying authentication mechanism, ABI can reduce delay and the probability of packets loss during both call initialization and HO processes, it can eliminate HO delay and minimizes resource possession during HO, enhance QoS in MRVSP and smooth HO procedure. ABI supports heterogeneous environments as well as a homogeneous network. Nevertheless, it will perform better in a network with QoS service. By modifying the details of this ABI scheme, it also can be used in other sceneries.

Acknowledgment

Project supported by the Provincial Natural Science Foundation of Fujian, China (No. 2012J01243, No.2012J01244), Fujian Province Industrial and commercial development Fund on enterprises technical innovation provincial project No.2011Four (One)52: "Intelligent Robots Storage systems research and development"; Project of Fujian Education Department (No.JA10216) and Fujian U. of Tech. Funds No.GY-Z10067 and No.GY-Z11065.

References

- [1] Upadhyay, P.C., Tiwari, S., IP Paging for Mobile Hosts in Distributed and Fixed Hierarchical Mobile IP. *International Journal of Wireless Networks and Broadband Technologies (IJWNBT)*. 1 (2011) 62-76.
- [2] Kim, S.G., Kim, D., Kim, J., Han, D., Park, B., A Novel Predictive Binding Update Scheme for Fast Handover over IP-Based Wireless/Mobile Networks. *Advanced Computer Science and Information Technology*. 195 (2011) 322-330.
- [3] Kim, S.C., Park, P.K., Moon, S., Shin, Y.S., Ryu, H.Y., Hong, S.B. Apparatus and method of controlling seamless handover between heterogeneous networks based on ipv6 over ipv4 tunneling mechanism. US Patent 20,120,014,350,2012.
- [4] Csaszar, A., Karagiannis, G., Marquetant, A., Partain, D., Pop, O., Rexhepi, V., Szabo, R., Takacs, A., Westberg, L., Resource Management in Diffserv (RMD): A Functionality and Performance Behavior Overview. *IFIP Lecture Notes in Computer Science (LNCS)*. 2334 (2011) 17-34.
- [5] Bournelle, J., Giaretta, G., Nakhjiri, M., Tschofenig, H., Korhonen, J. Diameter Mobile IPv6: Support for Home Agent to Diameter Server Interaction. *IETF RFC 5778*, February 2010.
- [6] Jang, H.J., Han, Y.H., Jee, J., Park, S.D., Cha, J. Mobile IPv6 fast handovers over IEEE 802.16 e networks. *IEEE RFC5270*, 2008.
- [7] Zhang, Y., Jiang, X., Luo, L. Trigger Mechanism of Context Transfers in Seamless Handovers for Multimedia Applications. in: *International Conference on Communication Technology*, IEEE, Gulin, 2006, pp. 1-4.
- [8] Chaudet, C., Chelius, G., Handoff Notification in Wireless Hybrid Networks. *IFIP Advances in Information and Communication Technology (AICT)*. 162 (2011) 47-58.
- [9] Benoubira, S., Frikha, M., Tabbane, S., Mobility and QoS Management in Heterogeneous Wireless Networks. *IJCSNS*. 11 (2011) 82.