IMSI-BASED CARE OF-ADDRESS CREATION FOR FAST BINDING UPDATE IN MIPv6

Armanda Caesario Cornelis [1], Rahmat Budiarto[2], and Edwin Purwadensi[3]

[1]*School of Computer Sciences-Universiti Sains Malaysia, Malaysia, armand.caesar@gmail.com*
[2]*School of Computer Sciences-Universiti Sains Malaysia, Malaysia, rahmat@cs.usm.my*
[3]*Telkom Multimedia, P.T. Telekomunikasi Indonesia, Indonesia, Edwin@telkom.co.id*

ABSTRACT. The growth of Internet user forced the fixed line Internet user to migrate from IPv4 to IPv6 due to the address availability. The similar situation will arise in mobile Internet, in which will forced the users to migrate to IPv6-based network. The numbers of Internet user also affect the access router work load and may grounds the latency in data reception. Handover from one access router to another needs a mechanism called binding update which produces latency. The most liable process in this mechanism is Duplicate Address Detection (DAD) in which take longer time than any other process. This paper proposes a mechanism to reduce the handover latency by eliminating the DAD process, using IMSI number.

Keywords: Binding update, Duplicate Address Detection, handover, MIPv6, IMSI, FMIPv6

INTRODUCTION

Thomson (Thomson et al., 1998) introduced a mechanism to avoid IP address duplication on the network called Duplicate Address Detection (DAD). This mechanism is performed on unicast addresses and must take place on all unicast addresses, regardless of whether the addresses are obtained through stateful, stateless or manual configuration. RFC 2462 stated that DAD may not perform in two cases:

- On anycast addresses.
- Each individual unicast address should be tested for uniqueness. However when stateless address auto-configuration is used, address uniqueness is determined solely by the interface identifier, assuming that subnet prefixes are assigned correctly.

In case a duplicate address is discovered during the process, a new identifier will be assigned to the interface or all IP address for the interface will need to be manually configured. When DAD is applied to addresses, it will be considered as tentative until the procedure has completed successfully.

The address duplication may occur when a mobile node proposes an address to the New Access Router (NAR). Even the address itself is formed by NAR prefix, the interface identifier which is proposed by the mobile node could be the same. Fundamentally the Mobile IPv6 (MIPv6) and Fast Mobile IPv6 (FMIPv6) already provided alternative address in case the duplication is detected. However the alternative address itself might have duplication on the network. The DAD mechanism may take longer time if this happened.

RELATED WORKS

MIPv6 (Mobile IPv6)

MIPv6 is the model of mobility support for IPv6. This model (Johnson et al., 2004)consists of four entities: the Home Agent (HA), Mobile Node (MN), Correspondent Node (CN) and Access Router (AR).The Home Agent function is to assign MN a home address which serves as home origin identification. All data from Correspondent Node is routed to MN via Home Agent if MN is still in Home Agent area, but when MN roams to foreign area FA is responsible to route the data from Correspondent Node. However, the MN has to be authenticated first before receiving a temporary address called Care of Address (CoA) which provided by the FA.

FMIPv6 (Fast Handover Mobile IPv6)

FMIPv6 proposed by Koodli (Koodli, 2009) uses an approach to reduce the handover latency by managing the movement detection and early handover signaling. FMIPv6 model uses the PAR (Previous Access Router) and the NAR (New Access Router) to connect nodes. The PAR is a node where MN is currently attached. Before performing a handover process Correspondent Node sends packets to MN through the PAR node and vice versa. Once MN requesting a handover the PAR node creates a tunnel to the NAR in order to send the current packets from Correspondent Node, and NAR buffered the packets temporarily until the MN completely attached to the NAR. In FMIPv6 model the MN has to be verified by the home agent first before can proceed to the Correspondent Node's binding update. This sequence procedure (Binding Update to home agent then to correspondent node) produces multiple latencies.

The International Mobile Subscriber Identifier (IMSI)

The IMSI (Swenson et al., 2005, Bhattacharjee) is a unique identification number which linked with the Global System for the Mobile communication (GSM) and Universal Mobile Telecommunication System (UTMS) network. IMSI is stored as a 64 bit in the Single Identity Module (SIM) and usually has 15 digits length, but it is possible to use shorter length. IMSI contains Mobile Country Code (MCC), Mobile Network Code (MNC), and the Mobile Station Identification Number (MSIN). As shown in Figure 1 the IMSI format consists of three digits of MCC, two digits of MNC and ten digits of an identification number.

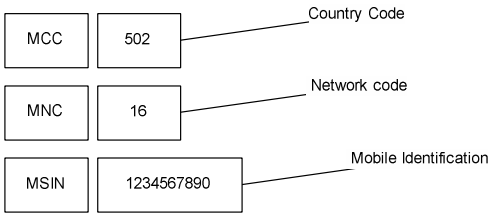

Figure 26. IMSI format

The IMSI provides other details of the mobile within the Home Location Register (HLR) or as locally copied to the Visitor Location Register (VLR). The IMSI may provide the home network location of mobile station, when user is roaming in foreign network.

IMSI-BASED CARE of-ADDRESS CREATION

Basically in all MIPv6 based protocols the CoA is formed by the [AP-ID, AP-INFO] tuple (Johnson et al., 2004) as a subnet prefix and a random generated interface identifier (the last 64 bit after subnet prefix in IPv6 address). Therefore the Duplicate Address Detection model needs to be performed to obtain a unique CoA IP address.

The main concern in the DAD is related with CoA creation. The uniqueness of interface ID determines the CoA's uniqueness, this is because the n-bits of subnet prefix always uses the Access Router local link. IPv6 unicast address uses interface ID to identify interface on a link. The interface ID is illustrated in Figure 2.

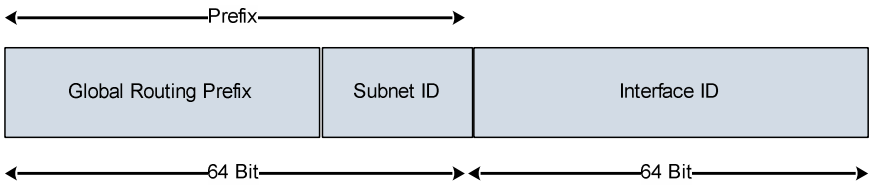

Figure 27. CoA Address

The proposed mechanism no need to perform the DAD process, because the Care-of Address (CoA) is formed by using [AP-ID, AP-INFO] tuple which the AP-ID part is given by Proxy Router Advertisement (PrRtAdv) and the AP-INFO part is generated by the IMSI. This model assures the Interface ID's uniqueness.

The IMSI number is provided by Subscriber Identity Module (SIM), known as Universal Integrated Circuit Card (UICC) in UMTS, and Removable User Identity Module (R-UIM) in CDMA. The creation of Interface ID is explained as follows.

The IMSI consists of 15 digits. The IMSI number of the mobile device should be translated into binary to fulfill the 64 bits interface identifier as a part of IPv6 address. So the 15 digits of the IMSI is represented by ((15 x 4) + 4= 64 bits) hexadecimal to ensure the uniqueness of interface ID and is used to formed the CoA. In Figure 3 the given example of IMSI is 060-016-408641300.

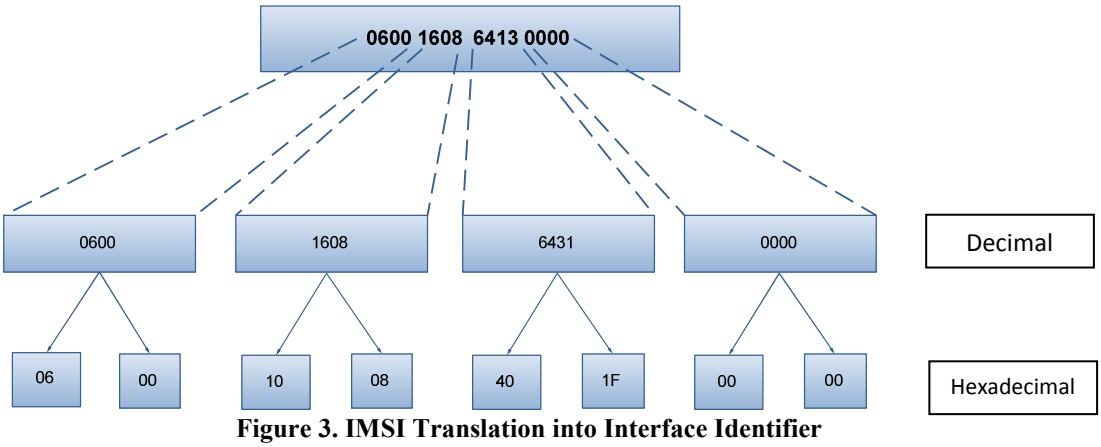

Figure 3. IMSI Translation into Interface Identifier

The translation is used for every four digits in decimal format which equal to 16 bits. For example we use the second four digits in the given IMSI number in Figure 3 which is 1608. First, we translate every two digits into hexadecimal (16 into 10) then continued with the next two digits (08 into 08). The completed creation of care-of address for the mobile node with the given prefix 2001 0DB8 85A3 FFFF is shown in Figure 4.

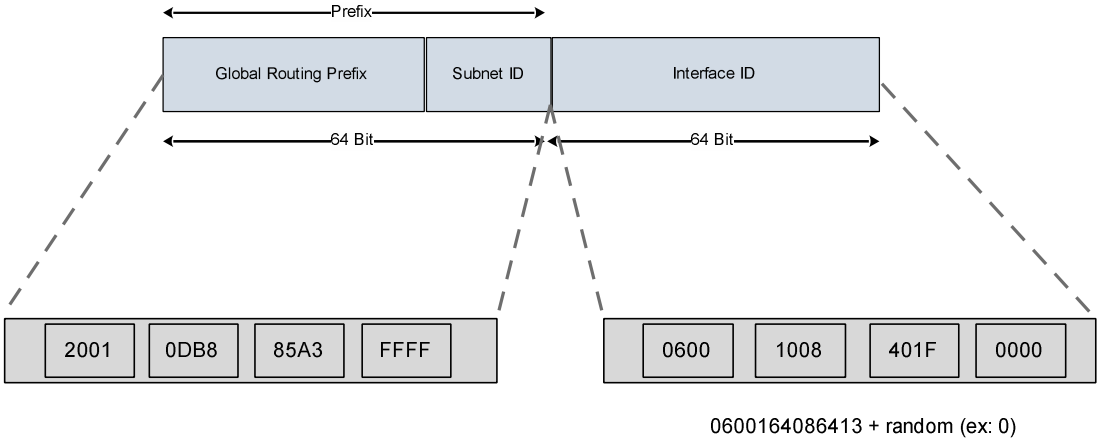

Figure 4. Care-of-Address forming

Once the CoA address is completely created, it can be immediately registered to the Home Agent and the Correspondent Node simultaneously. The CoA address will always become unique because the IMSI in every SIM card is always different yet it cannot be duplicated easily (Swenson et al., 2005).

SECURITY CONSIDERATION

The network provider originally has provided SIM with embedded authentication mechanism known as Authentication key (k_i). The k_i essentially is a 128-bit key that used by mobile network devices to authenticate the SIM. Each SIM has a unique key given by the mobile network provider at some points on personalization process at the beginning of registration on the mobile network service.

In real application the GSM cryptography has certain liability which may permit the extraction of the k_i from the SIM card and making a duplicate SIM card. To avoid this attack the provider may detect the fraud using Radio Frequencies Fingerprint (RFF) (Hall et al., 2005).

SIM clone attack on GSM technology can only be achieved by cloning the SIM card because the GSM phone does not have Electronic Serial Number (ESN) and Mobile Identity Number (MIN). Each mobile phone has a radio finger print in its transmission in which will remain unique despite it has the clone SIM. The mobile network provider may detect if there is any duplication occurs by comparing the RFF value (Hall et al., 2003).

Nowadays cloning the SIM card physically is almost impossible due to the embedded security system in the SIM card itself. Although the card successfully cloned, the forged SIM card cannot register to the network since the network will detect the two different location of SIM. Furthermore (Francis et al., 2010) proposed an embedded system to prevent hijacking which made the cellular device much more secure.

SIMULATION, RESULTS AND DISCUSSION

The FMIPv6 is considered faster than MIPv6 due to the temporary binding update in which allows mobile node to receive the data via data forwarding from PAR to NAR. Therefore we use the FMIPv6 as comparison for the simulation. We use the OMNET++ to simulate two models of the FMIPv6. The first one uses the DAD and the second one does not use the DAD. The simulation is conducted using the following mathematical model:

SC_x : Signaling Cost
T_{MP} : Packet delay between MN and PAR
T_{mn} : Packet delay between MN and NAR

T_{PM} : Packet delay between PAR and NAR in wired network
T_{new} : DAD latency, NCoA forming and so on.
T_{L3} : Time interval between the FBack received on the MN in PAR's link down.
T_{L2} : Link layer handover latency

$$SC_{FMIPv6\ IMSI-based} = 4T_{pm} + 4T_{mp} + BU_{CN} + BU_{HA} + 3T_{mn} \quad (1)$$
$$SC_{FMIPv6-\ DAD} = 4T_{pm} + 4T_{mp} + BU_{CN} + BU_{HA} + 3T_{mn} + T_{new} \quad (2)$$

Table 13. Average Handover latency

Handover	IMSI-Based FMIPv6	FMIPv6
1	1.03342221	1.165184
2	1.17689236	1.6800654
3	1.1805353	1.53957033
4	1.0051468	1.4523679
5	1.12594353	1.32641656
6	1.07777999	1.13353439
7	1.12345603	1.52614743
8	1.01281825	1.23721841
9	1.07272456	1.62268364
10	1.11693104	1.43253191
11	1.0860362	1.90776468
12	1.09805459	1.82401157
13	1.18120775	1.26715996
14	1.14331403	1.65163689
15	1.20093575	1.38609833
16	1.08150868	1.63915232
17	1.09687752	1.20610867
18	1.17989748	1.35786701
19	1.09627369	1.72433878
20	1.16359455	1.80250712
21	1.10554701	1.8512911
22	1.09129934	1.26042646
23	1.0475148	1.80311951
24	1.0758854	1.09594185
25	1.19301745	1.83935567
26	1.13864819	1.20308317

Handover	IMSI-Based FMIPv6	FMIPv6
27	1.10132009	1.45351258
28	1.01890202	1.71447376
29	1.0669737	1.80984714
30	1.02473235	1.91741215
31	1.10639593	1.92077072
32	1.10049534	1.16622477
33	1.17367566	1.27951072
34	1.07462367	1.82108677
35	1.11497363	1.88946151
36	1.15786377	1.32330058
37	1.03278763	1.3675107
38	1.10533115	1.17930364
39	1.13585967	1.97844208
40	1.08085522	1.53481326
41	1.06625376	1.69833492
42	1.12305398	1.92379483
43	1.16052816	1.8759107
44	1.10322325	1.60209932
45	1.03862007	1.78572516
46	1.06582052	1.85381515
47	1.1319531	1.88857111
48	1.00657478	1.67306949
49	1.07250797	1.32137332
50	1.19555083	1.66654106

Table 1 shows the linear movement handover completion time from 50 handover processes of the IMSI-Based FMIPv6 and the FMIPv6. As we can see from Figure 5 the IMSI-Based FMIPv6 always produces lower handover time compared to the FMIPv6. This fact shows that the IMSI-Based FMIPv6 handover process is faster than FMIPv6, which means IMSI-Based FMIPv6 efficiently reduces the handover processing time.

Figure 5 also shows that the average of handover completion time for the IMSI-Based FMIPv6 and FMIPv6 is 1.102781757 seconds and 1.629273966 seconds respectively. The IMSI-Based FMIPv6 manages to reduce the handover time by 63%. This fact indicates that the IMSI-Based FMIPv6 can reduce the handover time through implementing simultaneous binding update.

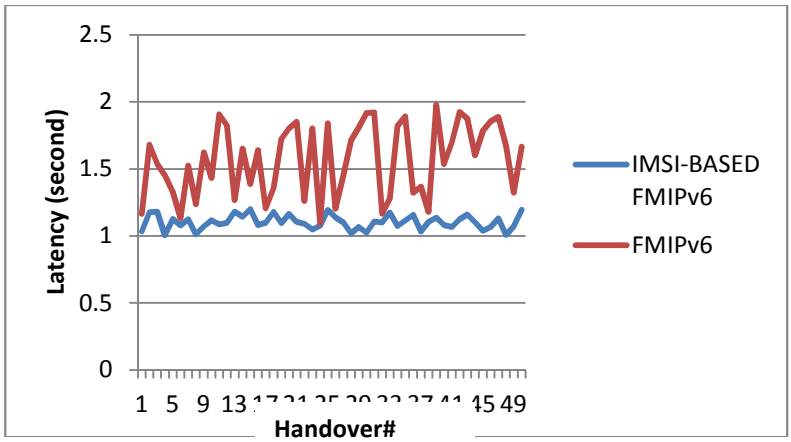

Figure 5. Handover Latency

CONCLUSION

The purpose of this paper is to propose an approach to reduce the handover latencies by eliminating the DAD procedure. The proposed mechanism ensures the uniqueness of an interface identifier by using the IMSI to create CoA for a mobile node in a subnet. The proposed mechanism is tested using mathematical model simulated in Omnet++ (Yousaf et al., 2008). In addition we compare it with the FMIPv6 and the result showed that the proposed mechanism is able to produce lower handover latency.

ACKNOWLEDGEMENT

This work is partially supported by the Fundamental Research Grant Scheme, Ministry of Higher Education, Malaysia as well as a Fellowship awarded to one of the authors by Universiti Sains Malaysia. The authors also would like to acknowledge the joint research collaboration with P.T. Telkom Indonesia that has resulted in this paper.

REFERENCES

FRANCIS, L., HANCKE, G., MAYES, K. & MARKANTONAKIS, K. Year. Potential misuse of NFC enabled mobile phones with embedded security elements as contactless attack platforms. *In*, 2010. IEEE, 1-8.

HALL, J., BARBEAU, M. & KRANAKIS, E. 2003. Detection of transient in radio frequency fingerprinting using signal phase. *Wireless and Optical Communications*, 13–18.

HALL, J., BARBEAU, M. & KRANAKIS, E. 2005. Radio frequency fingerprinting for intrusion detection in wireless networks. *IEEE Transactions on Defendable and Secure Computing*.

JOHNSON, D., PERKINS, C. & ARKKO, J. 2004. RFC 3775: Mobility support in IPv6. *Internet Engineering Task Force*.

KOODLI, R. 2009. Mobile IPv6 Fast Handovers. IETF RFC 5568, July 2009.

SWENSON, C., MANES, G. & SHENOI, S. 2005. Imaging and Analysis of GSM SIM Cards. *In:* POLLITT, M. & SHENOI, S. (eds.) *Advances in Digital Forensics.* Springer Boston.

THOMSON, S., NARTEN, T. & JINMEI, T. 1998. IPv6 stateless address autoconfiguration. RFC 2462, December 1998.

YOUSAF, F., BAUER, C. & WIETFELD, C. Year. An accurate and extensible mobile IPv6 (xMIPV6) simulation model for OMNeT++. *In*, 2008. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 1-8.