SeamSAR: Seamless, Secure and Robust Handover Model for Mobile IPTV Network Using Enhanced FMIPv6[*]

Ismat Aldmour[1], Thair Al-Dala'in[2], Lelyzar Siregar[3], Rahmat Budiarto[4]
[1,2,4]College of Computer Science & Information Technology, Albaha University, Albaha, Saudi Arabia
[3]Faculty of Computer Science and Information Technology, Universitas Sumatera Utara, Medan, Indonesia

Article Info	ABSTRACT

Multimedia becomes one of the most wanted content in the modern Internet world. Since the Mobile Internet Protocol version 6 (MIPv6) was proposed, many researchers have tried to develop a new protocol based on this technology in order to improve the performance of mobile multimedia services. The world is emerging toward the Mobile Internet Protocol Television (MIPTV) era where people are enabled to watch television while roaming. The MIPTV technology requires high bandwidth and low latency handover. This paper proposes a new model of secure and robust handover with low handover latency, called SeamSAR. The model introduces a new way to perform home binding update and correspondent binding update simultaneously. Simulation results show that the proposed model reduced the handover latency to 63% compared to FMIPv6. Moreover, the secureness of the proposed model was verified using CMurphi simulator.

Corresponding Author:

Ismat Aldmour,
Dept. of Computer Engineering and Science
College of Computer Science & Information Technology,
Albaha University,
 P.O. Box 1988 Albaha 65411, Kingdom of Saudi Arabia
Email: iaaldmour@bu.edu.sa

1.   INTRODUCTION

According to [1] most of mobile multimedia (e.g.: Mobile IPTV) technical obstacles are related to the wireless links. To guarantee the mobile IPTV works normally, a minimum bandwidth of 2-3 Mbps needs to be provided due to the characteristic of the mobile IPTV services. The limitations of wireless technology itself become problems in efforts to porting the traditional IPTV features into the mobile format. The most challenging yet disturbing limitation is the handover process, which occurs when users do a movement from one area into another area, especially that future networks will be characterized by frequent handovers due to the adoption of small cells. The handover process may disturb the reception of data and therefore it distresses the mobile IPTV users and produces undesired time improvidence.

Mobility in Internet Protocol version 6 (IPv6) is basic of upcoming services. Reducing the effect of handover potentially will reduce the data loss possibility and decrease the latency time.

Current protocols such as Fast Handover Mobile IPv6 (FMIPv6), Proxy Mobile IPv6 (PMIPv6), and Hierarchical Mobile IPv6 Mobility Management (HMIPv6) use the MAC address for authentication in their binding update processess to perform Duplicate Address Detection (DAD) process. In this process, the home agent binding update and corresponding node binding update process have to be done sequentialy. This work proposes the use of the International Mobile Subscriber Identity (IMSI) for the authentication process, as such we can perform the binding update processes concurently as shown in Figure 1.

---

[*]*This paper is an extended paper of the Int Conf on EECSI 2014*

This paper is organised as follows. Section 2 provides related works on handover protocols in mobile IPv6. Section 3 discusses the detail of the proposed enhancement of FMIPv6. Section 4 presents the experiment set up, results along with discussion. We conclude the paper in Section 5.
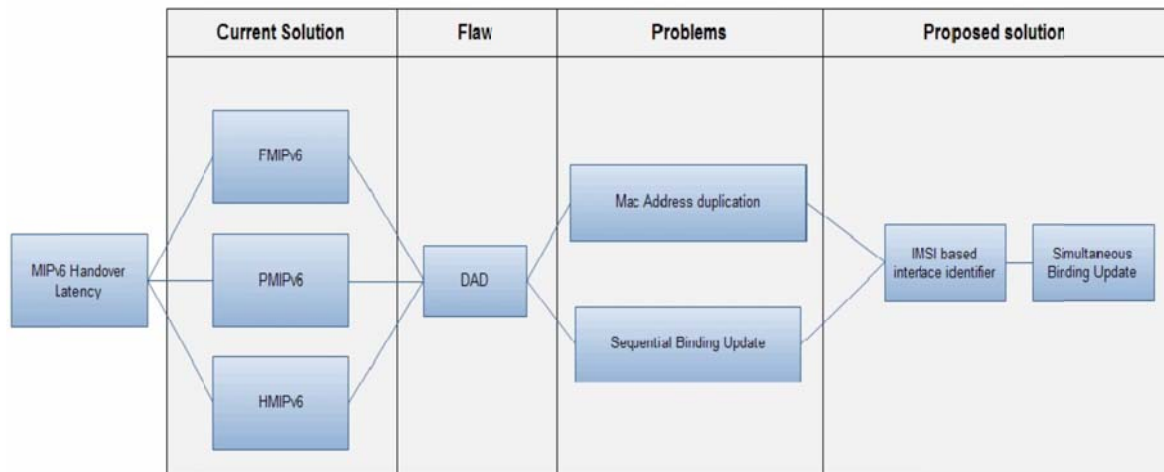

Figure 1. Schematic diagram of the proposed enhancement

2.   RELATED WORKS

MIPv6 defines an IP-layer mobility management scheme to provide Mobile Nodes (MN) with continuous Internet access while they move from one domain of Access Point (AP) to another. This process of changing AP is called handover. During this process the MN may be unable to neither send nor receive packets due to the delay of the handover process [2].

MIPv6 [3] consists of four entities: the Home Agent (HA), Mobile Node (MN), Correspondent Node (CN) and Foreign Agent (FA). The HA function is to assign MN a home address which serves as home origin identification. All data from CN is routed to MN via HA if MN still in HA area, but when MN roams to foreign area then the FA is responsible to route the data from CN. However, the MN has to be authenticated first before receiving a temporary address called Care of Address (CoA) provided by the FA.

FMIPv6 proposed by [4] and [5] uses an approach to reduce the handover latency by managing the movement detection and early handover signaling. FMIPv6 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 CN sends packets to MN through the PAR node and vice versa. Once MN requests a handover, the PAR node creates a tunnel to the NAR in order to send the current packets from CN, and NAR buffers the packets temporarily until the MN completely attached to the NAR.

The International Mobile Subscriber Identifier (IMSI) is a unique identification number that is linked to the Global System for Mobile communications (GSM) and the Universal Mobile Telecommunication System (UMTS) network. IMSI is stored as a 64 bit in the Subscriber Identity Module (SIM) and usually has 15 digits length, but it is possible to use shorter length [6]. In this paper, the Care-of Address (CoA) is formed by using [AP-ID, AP-INFO] tuple, where the AP-ID part is given by the Proxy Router Advertisement (PrRtAdv) and the AP-INFO part is generated by the IMSI. This model assures the Interface ID's uniqueness [7] (as shown in Figure 2).

Prefix

| Global Routing Prefix | Subnet ID | Interface ID |

64 Bit — 64 Bit

| 2001 | 0DB8 | 85A3 | FFFF |

| 0600 | 1008 | 401F | 0000 |

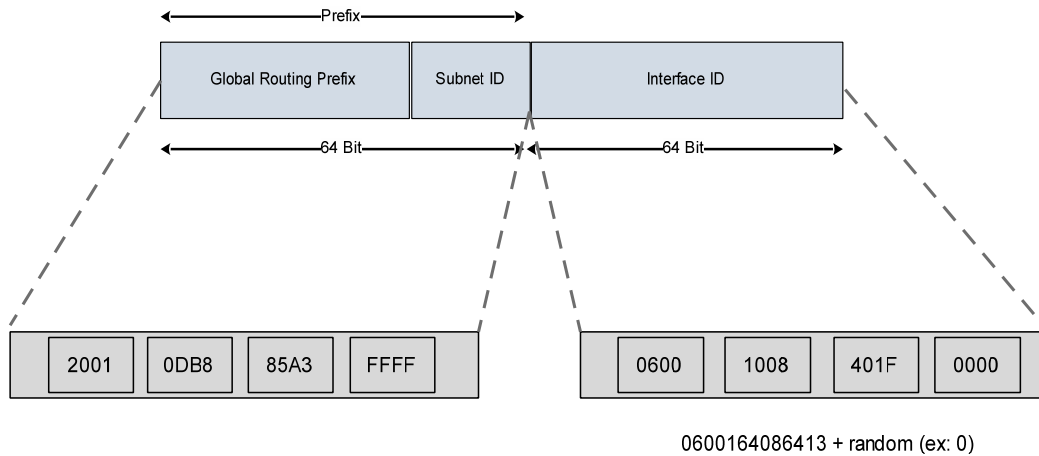0600164086413 + random (ex: 0)

Figure 2. Creation of Care of Address using IMSI [7].

Aldmour, et al., [8] enhanced the FMIPv6 by incorporating IMSI into the handover process and executing simultaneous binding update process.

3. THE SeamSAR MODEL

The proposed SeamSAR model shown in Figure 3 modifies the FMIPv6 operation during handover by sending concurently the Fast Binding Update (FBU) messages from MN to both HA and CN. Furthermore, the FBU message will be processed at nearly the same time at HA and CN. As soon as MN receives the beacon from the NAR, the MN sends the Router Solicitation to PAR and waits for Router Advertisement from PAR. After receiving the packet, MN sends the FBU packet to the PAR containing an interface ID generated from the IMSI number and a random number.

The FBU packet was forwarded to the HA in order to produce an early Binding Update for HA. The Binding Update process in CN can be done because at the time an FBU packet carries Home Test Initialization (HoTI) sent to HA, a Care of Test Initialization (CoTI) packet is sent from NAR to CN. As soon as the FBU packet is received by the HA, it continues to forward again the packet to CN to process once more as Binding Update for CN Binding Update.

Having received the FBU message, the PAR sends a Handover Initiate (HI) to NAR to start the FBU procedure. The FBU message contains the same message with the HI message that defined by FMIPv6. The PAR sends the acknowledgement packet called Handover Acknowledgement (HAck) to confirm the initiation process. Once the HAck packet is received by the PAR, it will send the FBU acknowledgement packet to both NAR and MN and start forwarding the packets from the CN to the NAR. In this step, NAR buffers the packets, so once the MN is attached to the NAR they can be delivered. This step has to be done to avoid the data loss and to make sure that MN gets the exact packets. Immediately after the PAR receives Binding Acknowledge message from the CN, the PAR starts to receive packets from CN, and the NAR stops forwarding the packets. MN starts to receive the packet right after the Unsolicited Network Advertisement is received by the PAR.

The FBU can be used by both CN and HA to initiate the Binding Update process because this message includes the prospective NAR address, which is generated by the MN using the information provided by the Router Advertisement message. This message has the same format of the ordinary Binding Update but provides a different mobility option, so basically it can be used by CN to initiate the binding update process. The HA sends a Binding Update message to the CN based on the FBU. As a result the MN does not need to send the Binding Update message to the CN. The registration time is considered as delay time. By processing this way the HA and the CN registration can be processed at the same time. Consequently, the delay time can be reduced.
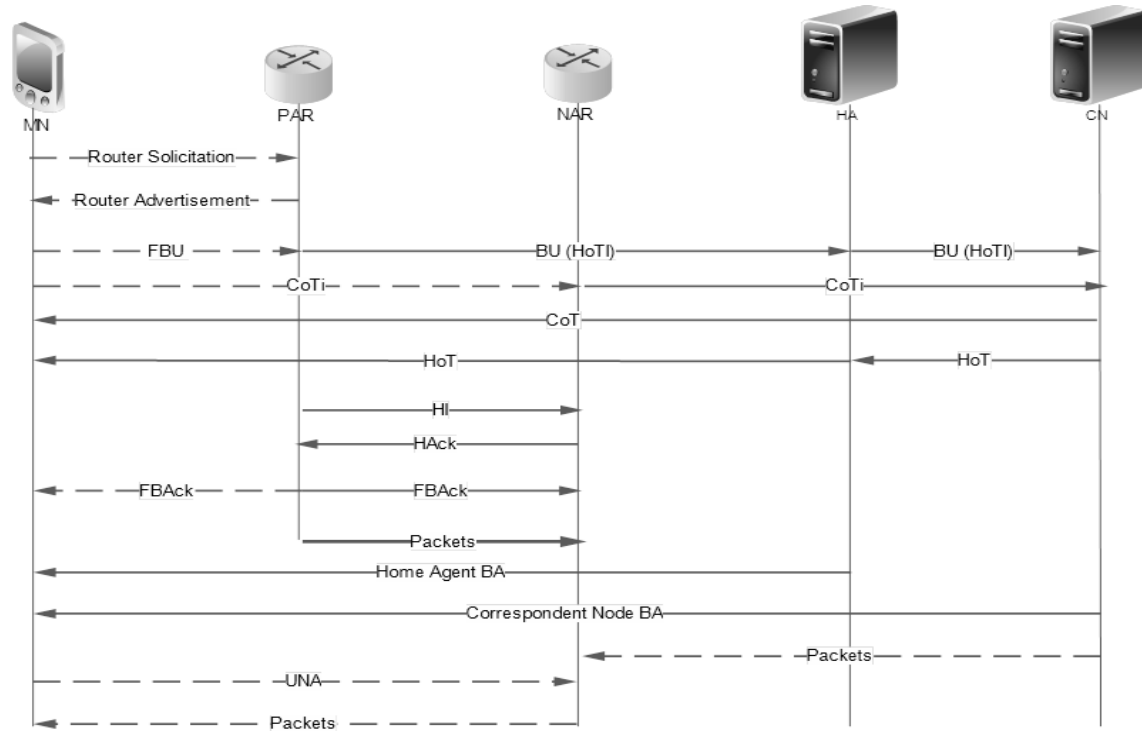
Figure 3. The SeamSAR Model

By implementing the IMSI-based interface identifier forming method, the Duplicate Address Detection (DAD) process can be removed. Hence the overall handover latency can be reduced. The proposed enhancement modifies the mobile IPv6 header format for the FBU to carry a HoTI Message, and an additional network advertisement packet sent to the NAR. The packet carried the CoTI packet will be forwarded to CN. As both HoTI and CoTI are received, CN can start the correspondent node Binding Update process. The modified FBU message contains a Home Init Cookie.

4.   EXPERIMENT AND RESULTS

We simulate both, the proposed SeamSAR and FMIPv6 using Omnet++ that has the ability to provide a real Mobile IPv6 environment [9]. We measure the dropped packet as well as the scalability of the processing time. The simulation topology consists of 3 access routers (Ars) and 1 access point (AP) as HA, 2 servers as CNs, and 1 MN. The MN increases up to 30 for the mass handover experiment. Table 1 shows the simulation paramenters. The MN is simulated as a node moving around while receiving IPTV streaming data. The topology of the simulation is shown in Figure 4.

Table 1. The Omnet++ Simulation Parameters.

| Entity	Parameter	Value
HA	IP address, SSID, Channel	10:AA::1:A0:1, HOME, 1
Access Router1	IP address, SSID, Channel	10:AA::1:A1:1, AP1, 2
Access Router2	IP address, SSID, Channel	10:AB::1:A2:2, AP2, 3
Access Router3	IP address, SSID, Channel	10:AE::1:A3:3, AP3, 4
MN	Speed, Mobility	1-20 mps, Rectangle, Turtle,
CN1	IP address	10:FF::A1:FF
CN2	IP address	10:FF::A2:FF
General	Neighbor Discov min. interval	0.03 s
	Neighbor Discov max. interval	0.07 s
	Packet Size	100 – 1024 Kb
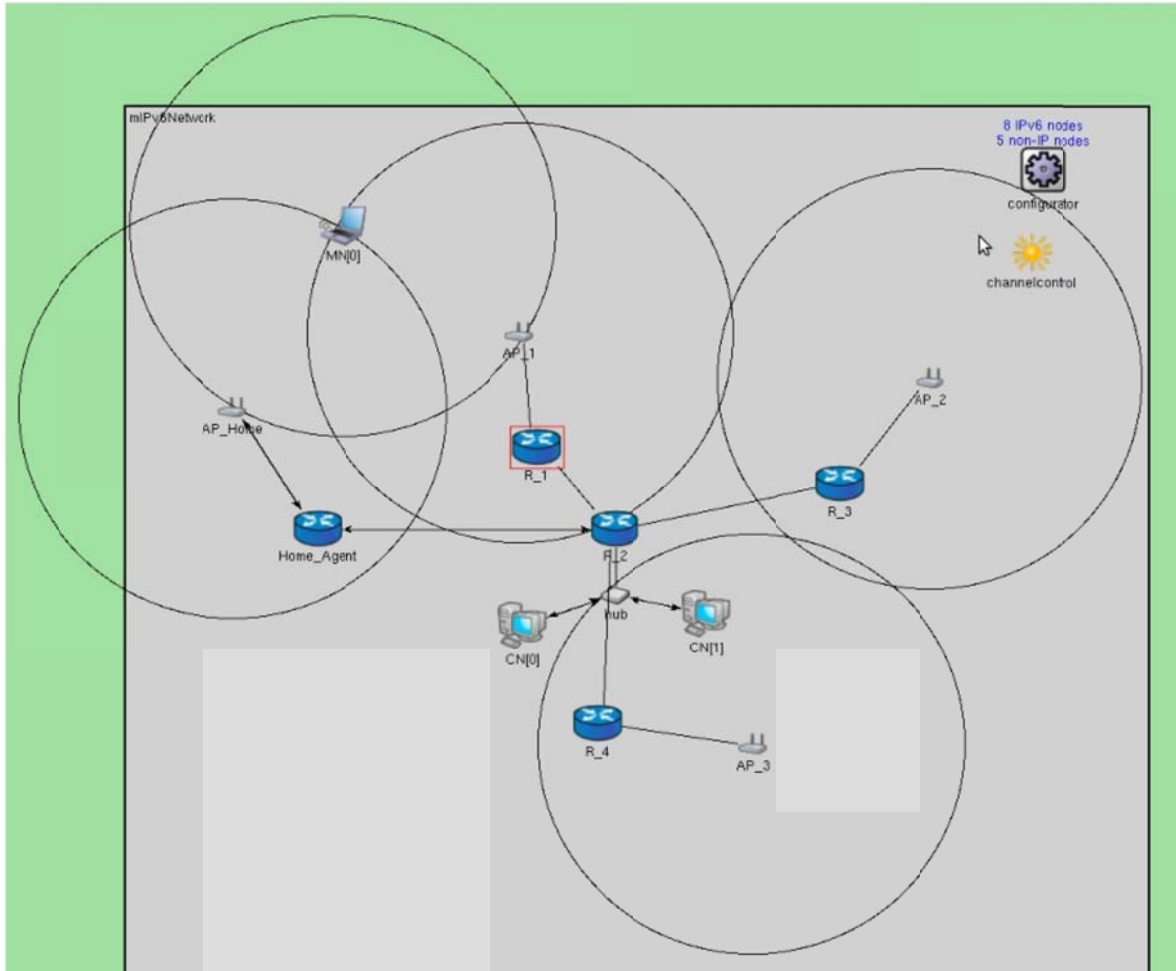
Figure 4. Omnet++ topology for the SeamSAR model

4.1. Packet drop

The packet drop may occur during the packet buffering in PAR. A neighbor discovery operation relating a neighbor's address resolution (i.e, Neighbor Solicitation and Neighbor Advertisement) usually results in considerable delay. We discover that the proposed enhancement and FMIPv6 have same packets drop rate of 6%. This fact shows that the capability to handle packet drop is the same as in FMIPv6.

4.2. Processing time latency

Figure 5 shows the average of handover completion times of FMIPv6 and the SeamSAR for various number of handover processes. From the figure, it can be seen that FMIPv6 requires longer time during the first handover, while the SeamSAR takes the shortest time which is 1 sec on the 5th and the 12th handover. This fact shows that the handover latency of the proposed enhanced FMIPv6 is stable and always below the latency of the MIPv6. The average Latency of the enhanced FMIPv6 and the FMIPv6 is 1.00250018 sec and 1.59127012 sec, respectively. Meaning that the SeamSAR reduces the latency by 37%.

4.3. Mass Handover Processing Time Comparison

To compare the performance of SeamSAR model and the FMIPv6 in terms of mass handover latency and scalability, we have put a scenario where 10 MNs request handover at the same time with different sizes of the packets, then we measured the handover processing time (latency) [10]. The results are shown in Figure 6, from which, it can be said that the enchanced FMIPv6 is scalable and produces a stable latency with increased number of packets. The scalability and stability of the proposed model prove its robustness.
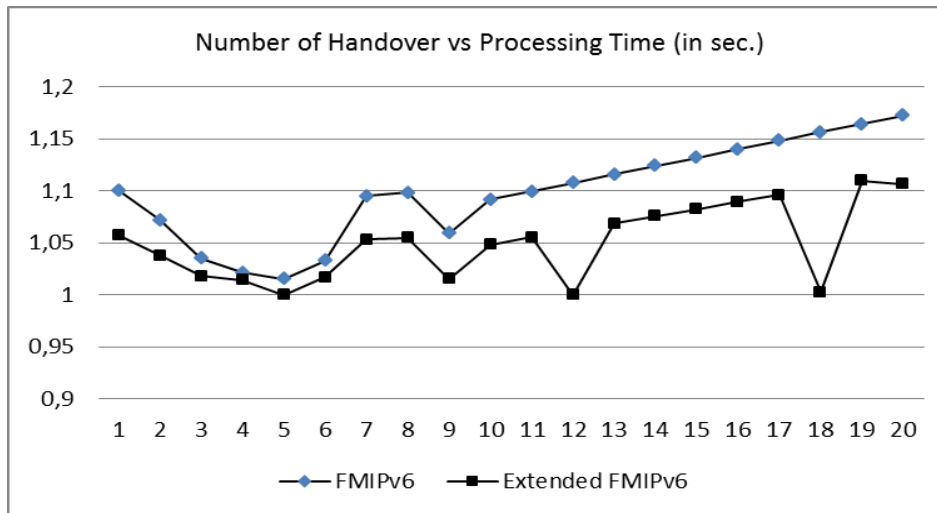
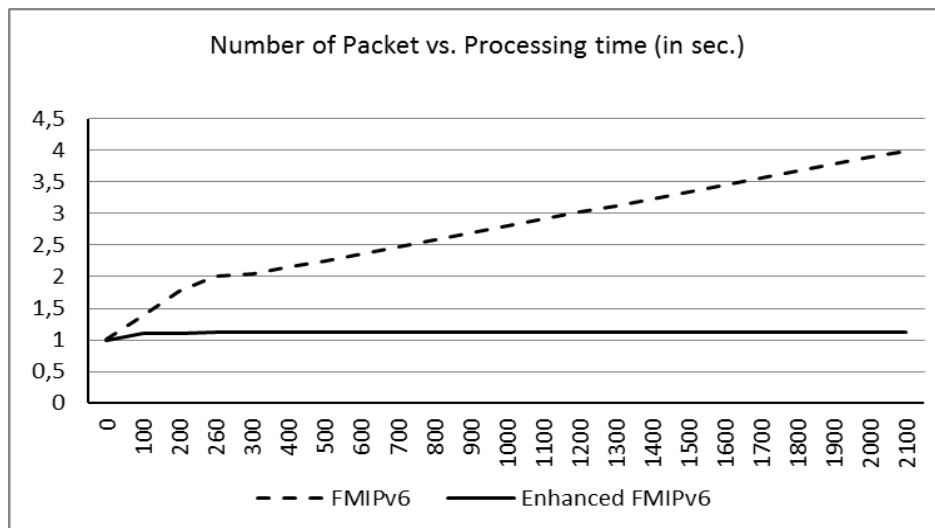Figure 5. Processing time for various numbers of handover processes in a router

Figure 6. Mass handover latency

4.4. Security Verification

Any mobility features is unsafe from misuse, and we have to protect it from possible threats. The main threat in handover model always involves the Binding Update packet. For instance, an attacker may impersonate a mobile node and act as Man-in-the-Middle, or other possibility is the malicious node may lure the correspondent node to send potential large amount of packets and causes the distributed denial of service. In order to make sure the SeamSAR is secure from such attacks we test the security aspect of the SeamSAR using the CMurphi finite state machine. Figure 7 shows a snapshot of overall CMurphi test results.

SeamSAR was tested for man-in-the-middle, eavesdrop, and impersonation attacks. The SeamSAR uses IMSI instead of MAC address, in which it is not possible for the attacker to fabricate the IMSI address of the mobile node. Thus, the attacker will fail to launch the attacks during the binding update process. In other word, the SeamSAR is robust against the three attacks.

```
=========================================================

Protocol: seamsar

Algorithm:
        Verification by breadth first search.
        with symmetry algorithm 3 -- Heuristic Small Memory Normalization
        with permutation trial limit 10.

Memory usage:

        * The size of each state is 760 bits (rounded up to 96 bytes).
        * The memory allocated for the hash table and state queue is
          8 Mbytes.
          With two words of overhead per state, the maximum size of
          the state space is 79687 states.
            * Use option "-k" or "-m" to increase this, if necessary.
        * Capacity in queue for breadth-first search: 7968 states.
            * Change the constant gPercentActiveStates in mu_prolog.inc
                to increase this, if necessary.

Warning: No trace will not be printed in the case of protocol errors!
         Check the options if you want to have error traces.

=========================================================

Result:

        Deadlocked state found.

State Space Explored:

        467 states, 930 rules fired in 0.10s.

Analysis of State Space:

        There are rules that are never fired.
        If you are running with symmetry, this may be why.  Otherwise,
        please run this program with "-pr" for the rules information.
        The maximum size for the multiset 'net' is: 1.
        The maximum size for the multiset 'int[IntruderId_1].messages' is: 1.
```

Figure 7. Snapshot of CMurphi Test.

5. CONCLUSION

We have proposed SeamSAR that enhanced FMIPv6 by introducing a concurrent HA and CN binding update process. The handover latency is reduced to 63% of the FMIPv6 latency. The security test using the CMurphi shows that the proposed SeamSAR model is robust against man-in-the-middle, eavesdrop, and impersonation attacks. With the lower latency and proper security, the proposed SeamSAR model may support mobile IPTV applications.

Further investigations on signal cost analysis of the proposed SeamSAR model will be considered as our future works.

REFERENCES

[1] S. Park and S. Jeong, "Mobile IPTV: Approaches, Challenges, Standards, and QoS Support," *IEEE Internet Computing,* vol. 13(3), pp. 23-31, 2009.
[2] V. Vassiliou and Z. Zinonos, "An Analysis of the Handover Latency Components in Mobile IPv6," *Journal of Internet Engineering,* vol. 3(1), pp. 230-240, 2010.
[3] D. Johnson*, et al.*, "RFC 3775: Mobility support in IPv6," IETF RFC 3775, 2004.
[4] R. Koodli, "Fast Handovers for Mobile IPv6 (FMIPv6)," IETF RFC 4068, July 2005.
[5] R. Koodli, "Mobile IPv6 Fast Handovers," IETF RFC 5568, July 2009.
[6] C. Swenson*, et al.*, "Imaging and Analysis of GSM SIM Cards," *Advances in Digital Forensics.* vol. 194, M. Pollitt and S. Shenoi, Eds.: Springer Boston, 2005, pp. 205-216.
[7] A. C. Cornelis, *et al.*, "IMSI-Based Care Of-Address Creation For Fast Binding Update In MIPv6," In: Proceedings of the 3rd International Conference on Computing and Informatics, pp. 321-326, 2011.

[8]   I. Aldmour, *et al.*, "Enhancement of FMIPv6 by Utilising Concurrent Binding Update Process", In: Proceedings of International Conference Electrical Engineering, Computer Science and Informatics (EECSI 2014), pp. 183-185, 2014

[9]   F. Yousaf, *et al.*, "An Accurate And Extensible Mobile IPv6 (xMIPV6) Simulation Model For OMNeT++," In: Proceedings of the 1ˢᵗ International Conference on Simulation Tools & Techniques for Communications, Networks, and Systems, pp. 1-8, 2008.

[10] X. Wu and G. Nie, "Performance Analysis and Evaluation of Handover in Mobile IPv6," In: Proceedings of IEEE International Symposium on Intelligent Ubiquitous Computing and Education, pp. 381-384, 2009.

BIOGRAPHIES OF AUTHORS

Ismat Aldmour received his PhD from the University of Glamorgan (currently University of South Wales) in Wales, UK, in the area of mobile wireless networks, in 2008. Both his MSc and BSc were from the university of Jordan-Jordan in the field of Electrical Engineering/ Communications. He is currently an assistant professor in AlBaha University in Saudi-Arabia in its Computer Engineering and Science department. His current research interests include resource management in future 5G networks, mobility management, WSNs and engineering education.

Thair Al-Dala'in is an Assistant Professor in the Department of Computer Science & IT at Albaha University, KSA where he has been a faculty member since 2012. Thair received his Ph.D. in Information Technology from the University of Newcastle in 2011. He completed his M.S. Degree in Computer Science at The University of Science, Malaysia in 2004 and his undergraduate studies at Mutah University, Jordan in 1997. His research interests lie in the area of E-Commerce Security, Network Security, and Trust in Social Network.

Lelyzar Siregar received her BSc in Computer Science from Gunadarma University in 1993 and Master of Computer Science from Gajahmada University in 2004. She is currently working with Faculty of Computer Science and Information Technology, Universitas Sumatra Utara, Indonesia. Her research interests include Future Internet, security in wireless networks and QoS

Rahmat Budiarto received B.Sc. degree from Bandung Institute of Technology in 1986, M.Eng, and Dr.Eng in Computer Science from Nagoya Institute of Technology in 1995 and 1998 respectively. Currently, he is a professor at College of Computer Science and IT, Albaha University, Saudi Arabia. His research interests include IPv6, network security, Wireless sensor networks and MANETs.