International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-2, December 2018

Protocol Converter between Mobile IP and WATM Wireless Networks

Dina M. Ibrahim

Abstract: ***This paper is concerned with the problem of designing and verifying internetworking protocol converters on the basis of timed Petri nets. The Petri net protocol conversion designated between the Mobile Internetworking Protocol (Mobile IP) and the Wireless Asynchronous Transfer Mode (WATM) protocol is investigated. Due to protocol complexity in this case, we propose a routing arrangement scheme for either protocol and for the intended protocol converter, in order to facilitate the derivation of the various traces involved. Petri net-based converter between Mobile IP and WATM protocols is constructed and verified. The converter is verified by simulation to guarantee liveness, safety, and responsiveness.***

Index Terms: Mobile IP, Petri Nets, Protocol Converters, Wireless Network Protocols

I. INTRODUCTION AND BACKGROUND

We are now living in an information age based primarily on computer networks as a result of the evolution of computer and communications technologies. The term computer network means a collection of autonomous computers interconnected by a specific technology. Due to protocol mismatch, we do need some sort of translation or interpretation for the protocols involved so that the networks can 'understand' each other. This process is known as *protocol conversion*, which implies constructing a converter as a *mediator* between two given protocols [1], [2]. It accepts messages from either protocol, interprets them, and then delivers appropriate messages to the other protocol.

The need for developing formal methods for protocol converter design was first pointed out by Green in 1986 [3]. His published work was the pioneering effort in the field of protocol conversion, where he defined the problem and stressed the need for facilitating interoperability between different network protocols [4], [5].

The protocol converter is designed in the following general successive phases:

- A Petri net model is constructed for each protocol through a particular number of stages, depending on the distinctive features and particular messages of the protocol. The construction process obeys an inside-out design strategy.
- The protocol model is verified by simulation using pertinent operating modes.

Manuscript published on 30 December 2018.
***** Correspondence Author (s)
Dina M. Ibrahim, Department of Information Technology, College of Computer, Qassim University, Qassim, Saudi Arabia.

- A synthesis procedure, relying on the concept of converter traces, is adopted to construct a Petri net model for the protocol converter between the two protocols at hand.
- The converter is verified by simulation to check three essential properties:

- Liveness: successful performance of the intended functions.
- Safety: disappearance of deadlocks and livelocks and satisfaction of place and transition invariants.
- Responsiveness: timeliness of function performing.

The complexity of the resulting protocol converter, estimated in terms of the numbers of places, transitions, arcs, and timers in the Petri net model, varies from one case to another according to the nature of the protocol.

II. MOBILE IP PROTOCOL

With the recent remarkable development of wireless technologies and very fast proliferation of mobile hosts it becomes a realistic scenario that mobile host users can freely move from one place to another while preserving communications [6], [7]. The Mobile IP protocol has been originally designed to support host mobility in the Internet. Eom et al. [8] develop a modified version of Mobile IP, and this will be used here. In the discussion to follow, we shed light on such a modification. In the base Mobile IP protocol, the Home Agent (HA) in the home network of the mobile host intercepts the packets destined for the mobile host, and then delivers them to the mobile host's current attachment point to the Internet using a tunneling technique [9], [10]. The current attachment point is defined by an IP address called a care-of address. This refers specifically here to a Foreign Agent (FA) care-of address; an address of an FA with which the mobile host is registered. When a mobile host (MH) moves into a new FA in a new network, it receives an agent advertisement message including the care-of address (*i.e.*, the address of the new FA) from the new FA [11]. At this time, the MH can realize that it moves into the new foreign network, and then sends the Registration Request (RegReqs) message requiring registration of the new care-of address to the new FA. The new FA relays it to the HA of the MH so that the HA delivers the packets to the new FA instead of the old one. In the route optimization extension, when the new FA receives the RegReqs message from the MH, it sends the Binding Update (BindUp) message to the old FA in order to inform the new care-of address, in addition to relaying the RegReqs message. Each time the old FA receives a packet from the corresponding host (CH), it has a responsibility to forward the packet to the new FA. In addition, it sends the Binding Warning (BindWar) message to the HA because the CH cannot know the new care-of address until the HA informs it.

When the HA receives the BindWar message, it sends the Binding Update (BindUp) message to the CH in order to inform the new care-of address.

After receiving the Bind Up message, the CH can send Packets to the new FA instead of the old one. By informing the Old FA of the new care-of address, the number of packets dropped during a handoff can be reduced because in general the New FA is likely to be farther from the HA than from the Old FA. This is called a seamless (or smooth) handoff.

The Mobile IP standard recommends to limit the maximum sending rate of the Agent Advertisement (AgentAdv) message to once per second for reducing the network load caused by the AgentAdv message. Therefore, even if the AgentAdv message is to be broadcasted at the maximum sending rate by the New FA, the MH cannot receive it during one second after moving into the new foreign network in the worst case. This means that during that time, in-flight packets destined for the MH are dropped because the MH cannot send the RegReqs message until receiving the AgentAdv message. For this problem, a local handoff protocol is incorporated in the route optimization extension as shown in Fig. 1. After receiving the Beacon message, which plays the same role as the AgentAdv message, the MH sends the handoff request (HO_Req) message to the New BS. The New BS then sends the Notification (Notif) message to the New FA for requesting the AgentAdv message.

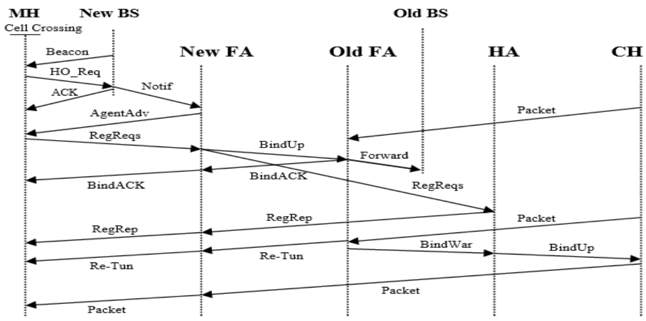

Fig. 1. Mobile IP with Route Optimization Extension to Support Buffering at BS

Upon receiving the Notif message, the New FA sends the AgentAdv message to the New BS. In this way, the MH can receive the AgentAdv message more quickly, compared to the method that periodically broadcasts the AgentAdv message to all of the BSs in the subnetwork. This is because the Beacon message used in the local handoff protocol is usually much shorter than the AgentAdv message and thus its sending rate is much higher than the maximum sending rate of the AgentAdv message. To facilitate the interpretation of Mobile IP communication messages, we propose the routing arrangement scheme established in Fig. 2.

The scheme consists of nodes and arrows. We have seven nodes representing MH, Old FA, New FA, Old BS, New BS, HA, and CH. Twenty named and numbered arrows connect these nodes together. The name of the arrow signifies the message and the number denotes its order in a time sequence. For example, the arrow designated '1. Beacon' refers to a Beacon message to be sent from New BS to MH as the first message in the sequence of messages, the arrow '2. HO_Req' refers to an HO_Req message to be sent from MH to New BS as the second message in the sequence, *etc*.

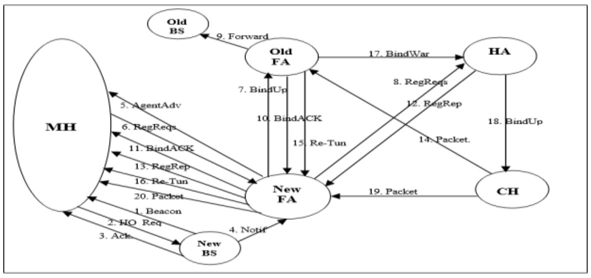

Fig. 2.Mobile IP Routing Arrangement Scheme

A. Construction of Petri net model for Mobile IP Protocol

In this subsection, a Petri net model of the Mobile IP protocol is constructed by using the routing arrangement scheme of Fig. 2. To this end, five consecutive stages constitute the construction process:

- Stage 1: fault-free situation (FF)
- Stage 2: MH lost-message situation (MHL)
- Stage 3: Old FA lost-message situation (OFAL)
- Stage 4: New FA lost-message situation (NFAL)
- Stage 5: timer representation (Tm)

An inside-out strategy is illustrated in Fig. 3 followed by the Petri net model of the Mobile IP protocol in Fig. 4.

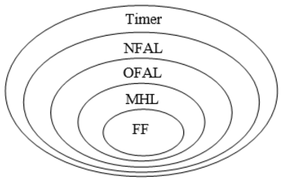

Fig. 3.Inside-Out Strategy for Mobile IP Model Construction

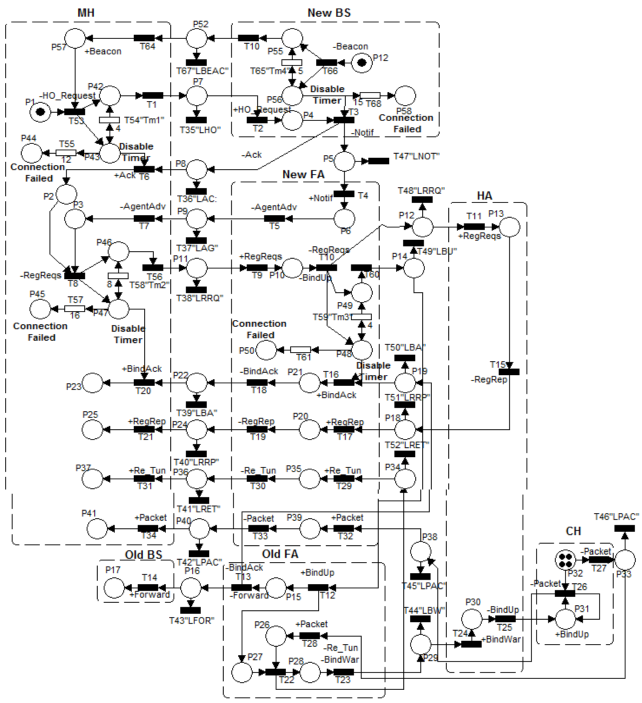

Fig. 4. Modeling result of Stage 5 (FF+MHL+OFAL+NFAL+Tm) of Mobile IP protocol (complete Mobile IP protocol)

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-2, December 2018

B. Verification of Petri Net Model for Mobile IP Protocol

The Mobile IP Petri net model established in the previous Subsection is to be verified. The HPSim software package is employed [12]. We have four operating modes:

- Operating mode 1: fault-free situation
- Operating mode 2: MH lost-message situation
- Operating mode 3: Old FA lost-message situation
- Operating mode 4: New FA lost-message situation

These operating modes correspond to Stages 1 through 4, respectively; the timer operation (corresponding to timer representation in Stage 5 of the construction process) is implied in the operating modes considered.

a. Verification of Operating Mode 1

In the fault-free situation, the steps traced are as follows. The New BS sends the Beacon message to the MH and starts the transmission timer Tm4 at the New BS. After receiving the Beacon, the MH sends the HO_Req to the New BS and starts the transmission timer Tm1 at the MH. After receiving the Ack, the MH disables timer Tm1. The New BS disables timer Tm4 after receiving the HO_Req and, then, sends a Notif message to the New FA, which sends the AgentAdv message to the MH. When the MH receives the AgentAdv, it sends the RegReqs to the New FA and starts the transmission timer Tm3. The New FA sends the same RegReqs message to the HA and sends the BindUp message to the Old FA and starts the transmission timer Tm2. When the New FA receives the BindAck message, it resends this message to the MH. After receiving the first Packet, the Old FA sends a BindWar message to the HA and sends a Re_Tun message to the New FA. When the CH receives the BindWar, it sends all the Packets to the New FA that resends them to the MH.

b. Verification of Operating Mode 2

In the MH lost-message situation, the simulation models of the token representing the HO_Req is moved to place P7. Transition T35"LHO" is fired to represent the lost HO_Req and, then, the token is removed from place P7.
Timer Tm1 expires and the MH resends the HO_Req two times without receiving Ack message from the New BS. Then, the MH disconnects by firing transition T55 which in turn disables timer Tm1. The MH receives the Ack and the AgentAdv messages and, then, sends the RegReqs by place P46 and a copy of this message is moved to place P47 to initialize timer Tm2. Transition T38"LRRQ" is fired to represent the lost RegReqs message and, then, the token is removed from place P11.

c. Verification of Operating Mode 3

For the representation of the simulation model of the Old FA lost-message situation, transition T49"LBA" is fired indicating that the BindAck message is lost. Timer Tm3, at the New FA, expires without receiving this BindAck and, then, the New FA resends the BindUp message to the Old FA, while timer Tm3 expires without receiving the BindAck from the Old FA. Then, the new FA disconnects by firing transition T61 that in turn disables the timer.

d. Verification of operating mode 4

To represent the simulation model of the New FA lost-message situation. Transition T49"LBU" is fired representing the lost BindUp and, then, the token is removed from place P14. If timer Tm3, in the MH, expires and no BindAck is received, the New FA expects that the BindAck is lost. Therefore, it sends a copy of the HO_Req again.

III. WIRELESS ATM PROTOCOL

Wireless ATM (WATM) is used for supporting multimedia services in mobile networks [13]. When a mobile user changes the access point, a handover is required to support a continuous communication service. Handover types can be classified into backward and forward handovers, depending on the way a handover is initialized and controlled. A backward handover is initialized and controlled through the old access point, whereas a forward handover is initialized and controlled via the new access point.

Handover types can be also classified into lossless and lossy handovers, according to whether or not cell loss is permitted during the handover. A lossless handover protects data integrity through preventing cell losses and guaranteeing cell sequence. On the contrary, a lossy handover permits some cell loss, yet it can support shorter handover delay and be less in complexity.

Here we use the WATM protocol presented by Kim and Cho [14], in which an inband-marking cell is used for minimizing cell losses. The Mobile Terminal (MT) sends the cross-over switch (CS) an inband-marking cell included in the disassociation procedure of a wireless link after data transmission through the backward link is finished [15].
Figure 5 shows the lossy handover procedure of the WATM protocol. We propose a routing arrangement scheme for this protocol, based on Fig. 5, as shown in Fig. 6.

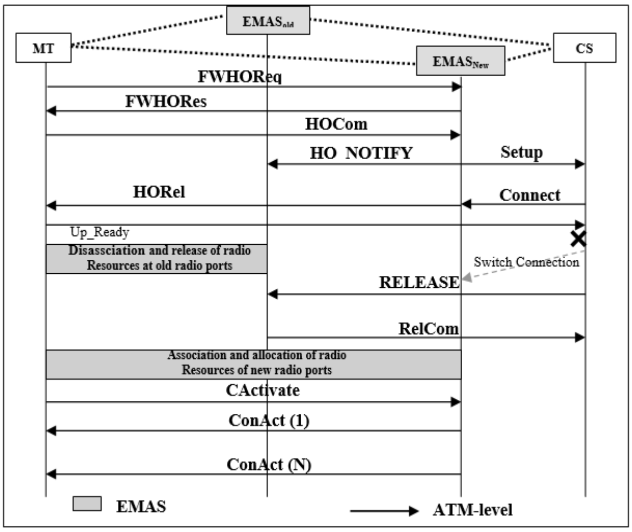

Fig. 5.Loosy Handover Procedure of WATM Protocol

The scheme consists of nodes and arrows. Four nodes represent MT, New End user Mobility Supporting ATM Switch ($EMAS_{NEW}$), Old End user Mobility Supporting ATM Switch ($EMAS_{OLD}$), and CS.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

These nodes are connected together with 14 named and numbered arrows.

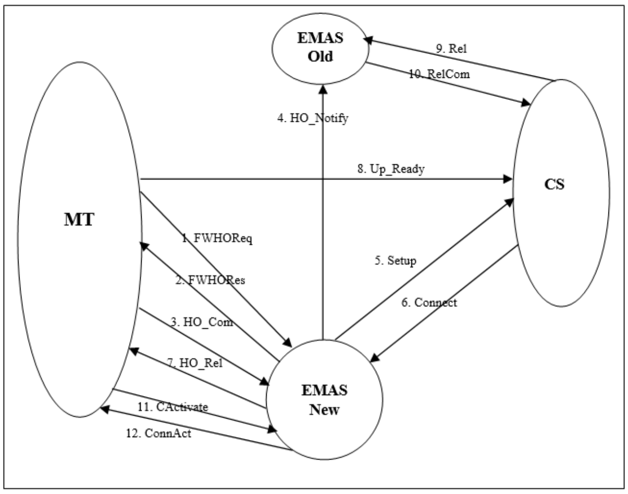

Fig. 6.WATM Routing Arrangement Scheme

A. Construction of Petri Net Model for Mobile IP Protocol

In this subsection, the WATM routing scheme of Fig. 6 is used to construct a Petri net model of the WATM protocol. Six consecutive stages constitute the construction process:

- Stage 1: fault-free situation (FF)
- Stage 2: MT lost- message situation (MTL)
- Stage 3: $EMAS_{OLD}$ lost-message situation (EMOL)
- Stage 4: $EMAS_{NEW}$ lost-message situation (EMNL)
- Stage 5: CS lost-message situation (CSL)
- Stage 6: timer representation (Tm)

Figure 7 illustrates the inside-out strategy followed by the Petri net model of the WATM protocol in Fig. 8.

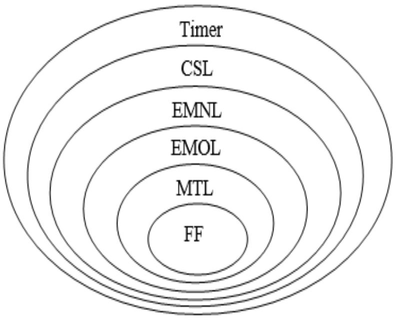

Fig. 7.Inside-Out Strategy for WATM Model Construction

B. Verification of Petri net model for WATM protocol

The WATM Petri net model founded in the previous Subsection is to be verified, through use of the HP Sim simulator. Five operating modes exist:

- Operating mode 1: fault-free situation
- Operating mode 2: MT lost-message situation
- Operating mode 3: $EMAS_{OLD}$ lost-message situation
- Operating mode 4: $EMAS_{NEW}$ lost-message situation
- Operating mode 5: CS lost-message situation

These operating modes correspond to Stages 1 through 5, respectively, in the construction process described above; the timer operation (corresponding to timer representation in Stage 6 of the construction process) is involved in the operating modes considered.

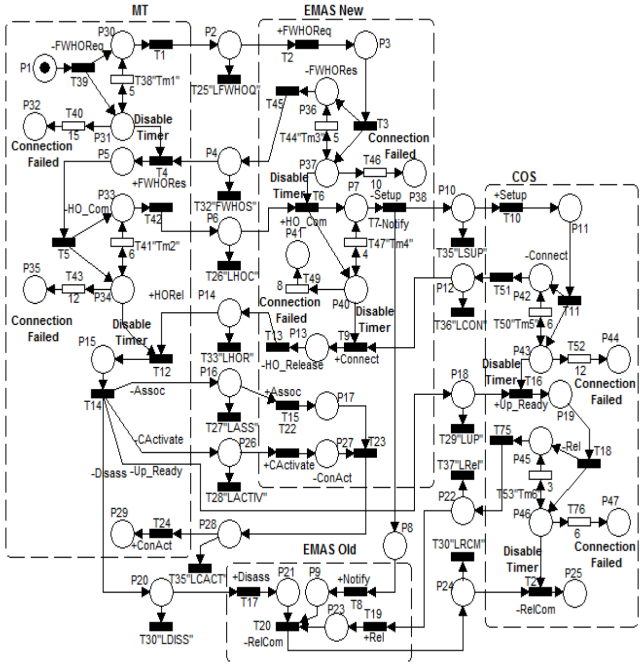

Fig. 8.Modeling result of Stage 6 (FF+M TL+ EMASOLD +EMASNEW+CS+Tm) (complete WATM protocol)

IV. PROTOCOL CONVERTER BETWEEN MOBILE IP AND WATM PROTOCOLS

The protocol converter between the Mobile IP protocol and the WATM protocol is now developed using the four-step synthesis procedure of III. The converter development includes two parts: in the first part, the Mobile IP protocol is a sender and the WATM protocol is a receiver while, in the second part, the WATM protocol is a sender and the Mobile IP protocol is a receiver.

A. Construction of Petri Net Model for Protocol Converter Between Mobile IP and WATM Protocols

To facilitate the formulation of the converter traces, we combine the Mobile IP routing arrangement scheme of Fig. 2 with the WATM routing arrangement scheme of Fig. 6. First, we treat the Mobile IP protocol as a sender and the WATM protocol as a receiver. Under this condition, we obtain a routing arrangement scheme for the converter between the two protocols as shown in Fig. 9. We have two nodes, MH and Old FA, from Fig. 2 and two nodes, $EMAS_{NEW}$ and CS, from Fig. 6. Three messages emanate from MH on the sender side to $EMAS_{NEW}$ on the receiver side. These messages are HO_Req on sender (FWHOReq on receiver), RegReqs on sender (HOCom on receiver), and CActivate. Three other messages go in the opposite direction: FWHORes on receiver (Ack on sender), HORel on receiver (BindUp on sender), and ConAct. A message BindAck emanates from Old FA to $EMAS_{NEW}$, and a message HO Notify on receiver (Bind Up on sender) goes in the reverse direction. Inside the receiver, a message Setup goes from $EMAS_{NEW}$ to CS, and a message Connect goes in the reverse direction. Likewise, when the WATM protocol is a sender and the Mobile IP is a receiver, we establish Fig. 10 by combining Figs. 2 and 6.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

We have three nodes, MT, $EMAS_{NEW}$, and CS, from Fig. 6 and three nodes, New FA, New BS, and HA, from Fig. 2. The messages between the different nodes are as given in Fig. 10.

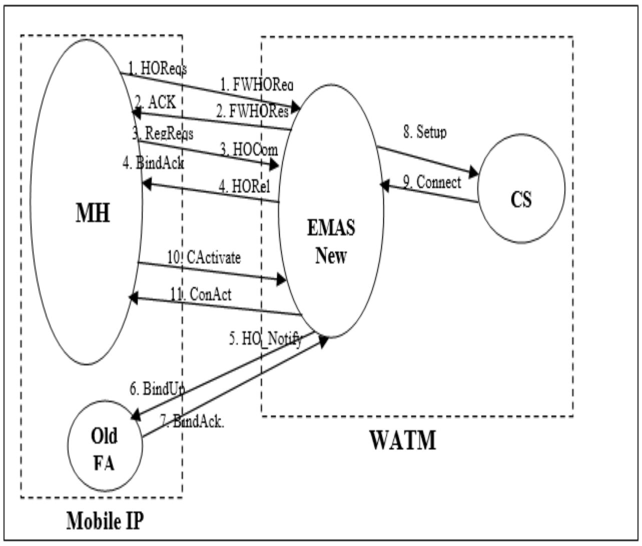

Fig. 9.Routing Arrangement Scheme for Converter between Mobile IP as sender and WATM as Receiver

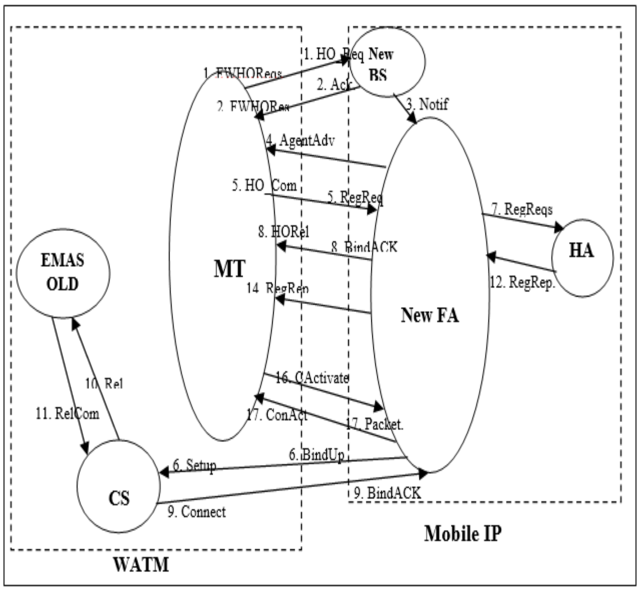

Fig. 10. Routing Arrangement Scheme for Converter between WATM as Sender and Mobile IP as Receiver

In Fig. 11, the Mobile IP protocol is a sender and the WATM protocol is a receiver. Four operating modes for the converter are represented in the model:

- MH lost-message situation
- Old FA lost-message situation
- $EMAS_{NEW}$ lost-message situation
- CS lost-message situation

The situation of New FA lost-message is not present because there is no NEW FA node to connect with the MH, whereas the two situations of $EMAS_{NEW}$ lost-message and CS lost-message are included because the MH needs to connect with nodes $EMAS_{NEW}$ and CS.

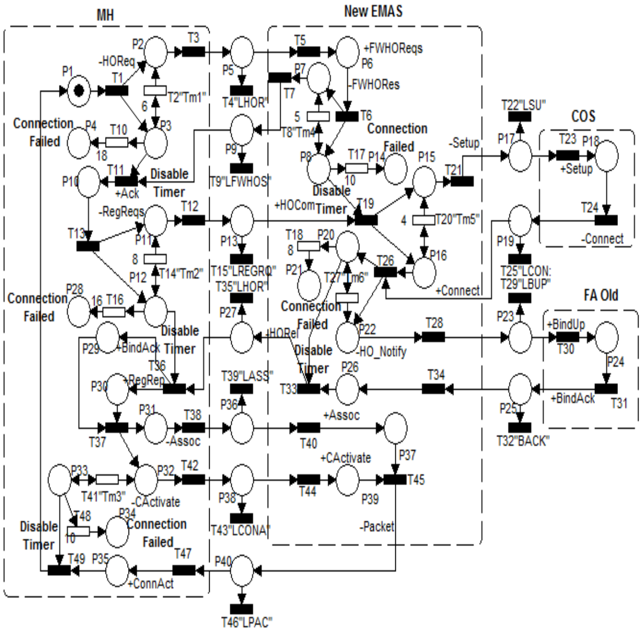

Fig. 11. Petri Net Converter Between Mobile IP as Sender and WATM as Receiver

In Fig. 12, the WATM protocol is a sender and the Mobile IP protocol is a receiver. Six operating modes for the converter are represented in the model:

- MT lost-message situation
- $EMAS_{OLD}$ lost-message situation
- New FA lost-message situation
- New BS lost-message situation
- HA lost-message situation
- CS lost-message situation

Fig. 12. Petri Net Converter Between WATM as Sender and Mobile IP as Receiver Organization of the Proposed Strategy Nodes.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

The situation of EMAS New lost-message is not present because there is no EMASNEW node to connect with the MT, whereas the situations of New FA lost-message and New BS lost-message are included because the MH needs to connect with nodes New FA and New BS.

B. Verification of Petri Net Model for Protocol Converter between Mobile IP and WATM Protocols

To verify the protocol converter constructed above, we use the HPSim simulator. We have to make sure that:

- The converter is live.
- The converter is safe.
- The converter is responsive.

Liveness of the converter: The converter liveness is verified through simulation of all possible operating modes. In the situation where the Mobile IP protocol is a sender and the WATM protocol is a receiver, there are four operating modes: MH lost-message, Old FA lost-message, $EMAS_{NEW}$ lost-message, and CS lost-message. In the situation where the WATM protocol is a sender and the Mobile IP protocol is a receiver, we have six operating modes: MT lost-message, $EMAS_{OLD}$ lost-message, New FA lost-message, New BS lost-message, HA lost-message, and CS lost-message.

Safety of the converter: The converter safety is demonstrated in the same ten simulation models used for verifying converter liveness. No state is reached from which no transition can be fired in the whole net and, furthermore, no state is reached from which the net cycles in a closed set of markings with no possibility of getting out of the cycle. This implies that our model is free from deadlocks and livelocks.

Responsiveness of the converter: The range of the internal timer Tm1 is from T_{min} = 6 sec to T_{max} = 18 sec. As an illustrative example, the situation of receiving an Ack message by the Mobile IP protocol, when the Mobile IP protocol is a sender and the WATM protocol is a receiver. It is obvious that the time required to receive this Ack message is exactly 6 sec – as specified. In the situation of lost Ack, the Mobile IP protocol resends the HO_Req message after 6 sec. The properties of liveness, safety, and responsiveness for the converter models are verified through simulation model.

REFERENCES

1. Lee, Y. M., and Park, K, H., A Protocol Converter for Nonblocking Protocols, INTEGRATION, The VLSI Journal, vol.33, pp. 71-88, 2002…..27
2. Saleh, K., and Jaragh, M., Synthesis of Communications Protocol Converters Using The Timed Petri Net Model, The Journal of Systems and Software, vol. 47, pp. 53-69, 1999. ….37
3. Green, P. E., Protocol Conversion, IEEE Trans. on Communications, vol. 34, pp. 257-268, 1986. …19
4. R. Sinha, "Conversing at Many Layers: Multi-layer System-on-Chip Protocol Conversion," *2015 20th International Conference on Engineering of Complex Computer Systems (ICECCS)*, Gold Coast, QLD, , pp. 170-173, 2015. doi: 10.1109/ICECCS.2015.25
5. R. Narayanan and C. S. R. Murthy, "A Probabilistic Framework for Protocol Conversions in IIoT Networks With Heterogeneous Gateways," in *IEEE Communications Letters*, vol. 21, no. 11, pp. 2456-2459, Nov. 2017. doi: 10.1109/LCOMM.2017.2730859
6. Siddiqui, F., and Zeadally, S., Mobility Management Across Hybrid Wireless Networks: Trends and Challenges, Computer Communications Journal, pp. 1-23, 2005…..39
7. Andrews, J. G., Ghosh, A., and Muhamed R., 'Fundamentals of WiMAX: Understanding Broadband Wireless Networking,' Prentice Hall, 2007.
8. Eom, D. S., Lee, H., Sugano, M., Murata, M., and Miyahara, H., Improving TCP Handoff Performance in Mobile IP Based Networks, Computer Communications Journal, vol. 25, pp. 635-646, 2002. ….13
9. S. N. Mane, N. V. Mane and D. G. Khairnar, "Performance of mobile node between different MANET with Mobile IP," *2015 International Conference on Industrial Instrumentation and Control (ICIC)*, Pune, pp. 1662-1664, 2015. doi: 10.1109/IIC.2015.7151017
10. O. Arafat, M. A. Gregory and M. M. A. Khan, "Interworking architecture between 3GPP IMS, Mobile IP and WiMAX in OPNET," *2014 2nd International Conference on Electrical, Electronics and System Engineering (ICEESE)*, Kuala Lumpur, pp. 48-53, 2014. doi: 10.1109/ICEESE.2014.7154602
11. M. Alnas, I. Awan and D. R. Holton, "Handoff mechanism in Mobile IP," *2009 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, Zhangijajie, pp. 176-179, 2009. doi: 10.1109/CYBERC.2009.5342167
12. Anschuetz, H., HPSim, Petri Net Simulator, Version 1.1, available on: http://www.winpesim.de/default.html, 2011.
13. S. V. Vambase and S. R. Mangalwede, "ATM based WMN architecture for Distributed Generation systems in electrical networks," *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, Noida, pp. 119-123, 2015. doi: 10.1109/ICGCIoT.2015.7380441
14. Kim, D., and Cho, Y., A Lossy Handover Scheme in The Wireless ATM Networks, Proceedings of IEEE, pp. 52-57, 2000.
15. Crazzolara, F. and Winskel, G., Petri Nets with Persistence, Electronic Notes in Theoretical Computer Science (Journal), vol.121, pp. 143-155, 2005.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)