Handover Delay Reduction Techniques over IP Network

Mohammad Nowsin Amin Sheikh, Nazmul Hossain, Md. Arif Rahman, Saumendu Roy

Abstract— Current mobile trend is based on Seamless communication and wireless network. Using one core IP network to roam among different networks is critical. That's why Seamless communication is an important research topic nowadays. The best successful solution is mobile IP. But the performance is poor considering the handover delay. Hierarchical MIP (HMIP) and Fast MIP (FMIP) are two standards for handover delay improvements. But still it can't fulfill the requirements. Thus combining intelligent algorithm of handover delay with tracking technology of movement, Seamless MIP(S-MIP) is came under consideration. In this paper, handover delay reduction approaches are shown first. We consider Seamless Mobile IP and study the effect in delay and performance. A simulative comparison is shown here in terms of handover delay, bandwidth and loss of packets. Simulation results are analyzed and S-MIP performances are evaluated. Proving suggestion of some future work the thesis concludes.

Index Terms— ARP, COA, Mobile IP, MIPv4, Handover Delay, MIFA, Seamless MIP and MAP.

1 Introduction

Technology of modern network firstly attained in the wired networks and the following engrossed in the field of wireless network. Applications may be worked in secure wired network, hybrid network or genuine wireless network. Progressing accomplishment or performance in these infrastructures (network) has been consecutive endeavor for decades. In this paper we have discussed about the approaches of the delay of handover reduction particularly, the Fast MIP (FMIP), Hierarchical MIP (HMIP) and Seamless Mobile IP. The paper discloses the effects of these intercourses in the network perfection and the handover delay as well. A study of simulation takes place an analogy among the bandwidth requirement, handover delay and packet loss. This paper finishes with the result of simulation analysis and lastly provides some suggestions for the work of future.

2 Overview of Mobile IP Protocol

In this section, we describe the Internet Protocol and different mobile IP version.

Internet Protocol: The Internet protocol (IP) gives an uncertain, connectionless delivery mechanism. It prescribes the fundamental unit of data alteration or transfer through TCP/IP [1]. IP executes the routing function, selecting a way for transmitting data. IP covers the law for the unfaithful data delivery: how routers and host mode packets, when and how error messages should be created, and which postulate can be cancelled. IP is liable from internetwork, interconnects many networks (sub-networks) into the internet [2]. Finding the packets from different sources and rescues them to the correct target or destination. This needs advance knowledge about the network topology, the selection of the compatible path, and the evasion of congestion; this may be completed using the scheme of IP addressing. IPv4 and IPv6 addresses are 32 bits and 128 bits long comparatively [3]. Some are preserved for IPv4 address and some are address of link local addresses that are not identical and routable on the link. The IPv6 adjacent discovery protocol is a much advanced version of two IPv4 protocols, the ICMP router indication protocol [4] and the address resolution protocol (ARP).

The IPv6 main features are:

- The Hierarchical addresses, for reducing the size of routing table in the memory.
- The simple header, for routing process and more fast or quick forwarding.
- Security enhancement, including the availability of encryption and authentication.
- The assignment of dynamic addresses.

Mobile IP Version: The IETF drafted a solution for the mobility of internet officially called "IP mobility support" and folksy named mobile IP (MIP) [5]. The usual features include: subtlety transparency to application and the protocols of transport layer, interoperability with IPv4 (using the similar addressing design), security and scalability [6, 7]. The challenge of mobility is how the host will intercept its address while it's converting, without demanding routers for learning host-specific routes [8]. Mobile IP resolves this problem by granting the mobile node to catch two addresses together. The first is permanent and stable; it employed by the applications and the transport protocols. The second is moveable or temporary; it shifts as the mobile node steps and is tenable only while the mobile node travels a certain position. The mobile node gets the permanent address on its actual home network. Then it goes to an external network and gets the moveable or temporary addresses. After that, node (mobile) must transmit the temporary address to an agent (router) at the home network. The agent then will separate packets transmit to the mobile node's fixed address, and uses the technique of encapsulation to tunnel the packets to nodes (mobile) of temporary address. When the mobile node steps again, it gets a fully new temporary address, and sounds the home agent of its recent position. When the mobile node behind home, it must amalgam the home agent to close intercepting the packets. Fixed address of mobile is called the home address, because it is attributed by the home network, and it is a similar address such that one ascribed to a static node. When the node (mobile)

appends to a external network, it must gain the moveable address which is known as care of address (COA) with concretion to a router in the foreign network named the external agent; the node (mobile) must primary discover the external agent then amalgam the agent to gain the care of address. The COA is acted like any other address on the external foreign network. Discovering the external agent (foreign agent discovery mechanism) is made by means of the ICMP router finding process. Routers transmit an ICMP router declaration message periodically for each and others and a host dispatching an ICMP router solicitation to prompt for an advertisement, this process is called the Router discovery mechanism. The mechanism of foreign agent discovery added more information to the router discovery message named the extension of mobility agent. This will grant the foreign agent to announce its being and mobile node to appeal the advertisement. After the mobile node records with an agent on the external network, it must also records with its home agent appealing to move packets to it COA. The node (mobile) transmits registration requests to the external or foreign agent that moves it to the home agent. A node (Mobile) notifies with other nodes by using the following process: when the MN sends or transmits information to another node, the packets pursues the shortest way from the foreign network to the appointed destination. The reply may not follow the similar route, packets are sent to the mobile's home network first to home agent that has registered the mobile COA. Second the HA waylays the packets to differentiate its targeted address and then it encapsulates and adits the packets to the care of address. This COA on the outdoor datagram marks the foreign agent, which gets the packets from the home agent, de-capsulate them, and then checks its registered mobiles table, and finally sends the packets to the right node (mobile). When the MN (mobile node) goes to a foreign network and wants to cohere with another node near to the foreign network this reasons a delay problem called the triangular routing. Every packet sent to the mobile node visit across the internet to the mobile's home agent that onwards the packets back again at the foreign network. The puzzle can be solved using a host specific route, which can be propagating to the nodes near the FAs; this can boost eliminating the delay [9].

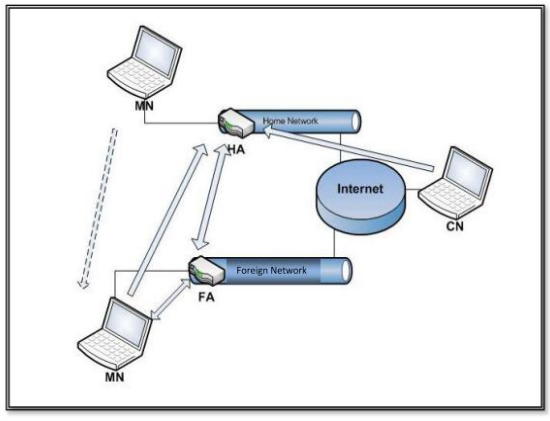

Fig. 1. Mobile IP Version 4.

Mobile IP Version 6: MIPv6 is the modified version of MIPv4, in order to match IPv6 requirements [10]. It has the same protocol architecture as MIPv4, with some differences in the foreign agent discovery procedure, COA (care of address) records, encapsulation and security enhancement. Three IPv6 addresses must be fixed to the mobile node that are the present link local address, the fixed home address and the care of address (COA) that is connected with the nodes of mobile home address, when it is travelling an external network. The network prefix of the COA will be the very similar to the foreign network prefix, and consequently all packets prescript to this COA will be immediately forward to the node (mobile). When the mobile node goes from one to another network, the care of address must be shaped by using temporary address auto configuration address (DHCP) according to the IPv6 adjacent unbolting protocol. The mobile nodes home address is associated with its COA known as binding; MIPv6 is managing a binding cache as an original data structure gathered by the node of each IPv6. After the node has fastened or registered to its COA with a home agent, the agent who uses proxy adjacent or neighbor discovery to separate IPv6 packets determined to the home address mobile node and mines them to the mobile nodes care of address by managing IPv6 encapsulation [9]. MIPv6 delivers the scope to other nodes to contact straightly the mobile node; a node of communicant will learn the knotting mobile node's, add these binding to the binding cache, and when it transmits packets to the mobile node, it shifts them to the mobile node's COA certain in the binding (this is same to the existing MIPv4 route optimization). In future, in order to contact with the node, the MN records its COA with its HA, and notifies correspondent nodes (CNs) with its binding to generate or update binding cache known as the update of binding. A binding confession is sent by a node showing that it gets the updating of binding. The acknowledgement of binding is transmitted directly to the mobile node, the goal address of the packets conveying the acknowledgement must be the nodes of mobile of COA which can be informed from the message of binding update. After receiving the update (binding) and registering it to the cache of obstructions, the informant node (CN) transmit packets straight away to the mobile node without the requirements of onward the packets, first is the mobile node's home agent. This process will aid to elect the triangular routing puzzle, which generates longer suspension to the packets delivery procedure [11]. A Mobile node must be able to transmit binding updates, execute IPv6 de-capsulation and receive binding acceptance. Similar rules apply to the correspondent nodes. In home network, the mobile node discovers new routers by using the protocol of router discovery appeared on obtained routers announcement messages. Discovery protocol of IPv6 neighbor is used by MIPv6 for motion detection as alluded before. Away from home, mobile node choose one router from the default (routers) list to be used as a default router, and when the router become inaccessible, mobile node must be switched to another default router. In wireless traffic, the mobile node is generally connected to the internet via various points of attachments or multiple entrance routers (wireless coverage overlap). The mobile node will take packets at its aged COA even after the

setup of its new COA and accusation it to the home agent; this makes the handover procedure smoother among the entrance or access routers. MIPv6 is more corroborating for security, using IPv6 some security specifications should be calculated; authentication required to be completed by all (IPv6) nodes, so the mobile node will be able to transmit authenticated binding updates. There is also extra overhead produced from the binding acknowledgement interchange. All this overhead will intuition the handover delay for mobile node while it's changing, and probably incrementing the handover delay.

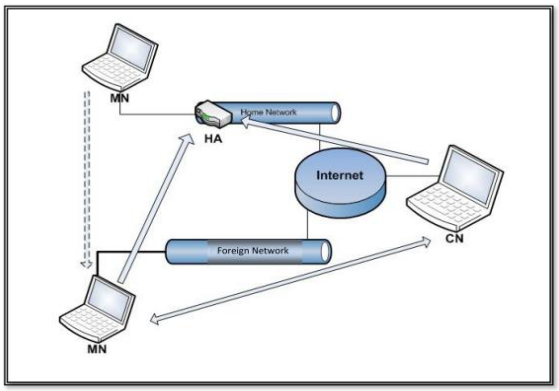

Fig. 2. Mobile IP Version 6.

3 HANDOVER DELAY APPROACH

3.1 Handover Delay reasons

A mobile node (MN) managing MIP to help mobility will execute different tasks exchanging information and signaling with the Home Agent (HA) and the Foreign Agent (FA): then it steps, a mobile node would detect that it has moved, communicate across the foreign network to gain a secondary address, and then communicate crosswise the internet to its home agent to manage packets forwarding. It demands considerable perfunctory after each step. Handover suspension or delay is the time that arrested for redirecting the continuous connection, when the mobile node transfers its attachment spot from one to another. The handover suspension is covered of two individual delays: First the time got for the HA registration procedure called as registration delay. Second the time that got for MN to configure a modern network COA in the foreign network named address resolution delay; both associated represent the bodily handover delay in mobile IP (MIP). Delay retrenchment solutions are principally navel to abate the FA address resolution delay and the HA registration delay. Hierarchical network construction approach is exposed to decrease the registration delay by using hierarchical handover. For address resolution delay, an address pre-configuration is published to reduce the delay time by fast handover access. A linked hierarchical and fast obtainment also is suggested to increase the perfection of mobile IP [12]. The presumptive handover suspensions are 300 to 400 milliseconds that are accomplished by numerous studies. This means that the packet loss for the IP layer handover procedure is still not enough to manage the original time applications.

3.2 Hierarchical Mobile IP (HMIP)

The hierarchical intercourse isolates the mobility aid management to micro mobility (intra domain) and macro mobility (inter domain). The node of mobile may move inside a appointed domain with no requirement to inform the Home Agent, as long as it goes inside that domain. A modern conceptual essence named Mobility Anchor Point (MAP) is used to help the hierarchical construction. MAP is a router that sustains the binding procedure with the mobile nodes currently travelling its domain. It is generally situated in the network's borders controlling numerous access routers, and get packets on behalf of the mobile nodes inside its domain. When the node (mobile) shifts to another network's domain it must register itself with the MAP serve that network domain [13].

The MAP function is to act as a Home Agent for the mobile nodes. So it separates the packets targeted to the address of mobile nodes inside its domain and then tubes them to the correspondent COA of the mobile nodes in their external network. When the node (mobile) changes it's care of address inside the MAP domain, it just requires registering this modern address with the MAP named Local care of address (LCOA). When mobile nodes move to a new MAP domain, it must attain a new regional care of address (RCOA) to get packets from outside the domain and also LCOA for inside domain movement. The mobile node would use the MAP's address as an RCOA, and it receives the LCOA from the Foreign Agent. After constructing the mobile node address transmits a binding update to the MAP, which will bind the mobile node's RCOA to LCOA. Then the MAP will transmit back a binding acceptance to the mobile node announcing the successful registration. Another binding update would be also transmitted to the mobile node's Home Agent every time it shifts its RCOA. Using HMIP; the mobile node just requires executing home agent registration when it shifts the whole MAP domain. As long as the mobile node goes inside the MAP domain, the HA registration will be concealed. This process will reduce the overall handover suspension by minimizing the HA registration delay [14].

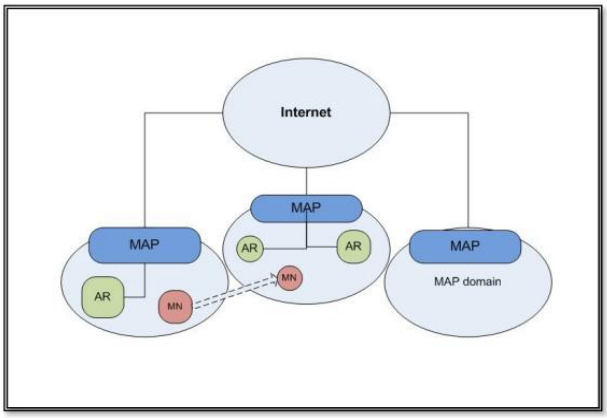

Fig. 3. Hierarchical Mobile IP.

3.3 Fast Mobile IP (FMIP)

The fast handover approach reduces the handover delay by reducing address resolution delay. The node of mobile will pre-configure a modern COA before it goes to a modern network. In the fast handover the node of mobiles shifts among access routers which defined as the last router connects the wired network to the wireless network. The old access router (OAR) is the router to which the node (mobile) is currently connected, and the new access router (NAR) is the router that the node (mobile) is planning to move. Fast handover uses the wireless link layer (L2) trigger which informs the mobile node that it will soon need to perform a handover. The L2 indication mechanism predicts the mobile node's movement according to the received signal power. Seven additional messages between the mobile node and the access router must be introduced by the fast handover: the Router Solicitation for Proxy (RTSO1PR) from the MN to the OAR, the Proxy Router Advertisement (PRRTADY) from the OAR to the MN, Handover Initiation (HI) from OAR to NAR and Handover Acknowledgement (HACK) from NAR to OAR. Besides Fast Binding Acknowledgement (F-BACK), Fast Binding Update (F-BU) and Fast Neighbor Advertisement (F-NA). To initiate a fast handover process in a wireless LAN first the node (mobile) transmits RTSO1PR message to the OAR after it notices the need for a handover; the address of link layer is sent to the next access node by the MN with RtSolPr message. The OAR response with PrRtAdv message, which contains some information about the new point of attachment if it is: known, unknown or connected to the similar to the mobile node the network prefix that should be used to create the modern or new care of address. After forming the new COA using stateless address configuration, mobile node transmits fast binding update (F-BU) to the OAR as the last message before acting the handover, and then a fast binding acknowledgement (F-BACK) will be sent either by the OAR or the NAR to the mobile node to insure a successful binding, the OAR will send duple F-Back messages to the NAR as well. When the mobile node shifts to a new network, it transmits a fast neighbor advertisement (F-NA) to initiate the packets forwarding from the NAR [15].

To facilitate packet forwarding, OAR and NAR will exchange some messages between them, which result in reducing the address resolution delay. The OAR sends a handover initiation message (HI) to the NAR, requesting a new COA registration for the mobile node and also it contains the old mobile nodes COA. The NAR will response by sending handover acknowledgment (Hack) to declare receiving or rejecting the modern COA. Temporary tunnel will be set by the OAR to the new COA if the NAR accepts the new COA. Otherwise the OAR will tunnel the packets to the NAR temporarily if it rejects the new COA, which will take care of forwarding the packets to the node (mobile). More than one study shows that using hierarchical and fast mobile IP together will effectively reduce the overall handover delay to around 300 to 400 milliseconds, which is still not sufficient for offering seamless handover requirements [16].

3.4 Seamless Mobile IP (S-MIP)

The architecture of seamless handover which is based on both a fast handover algorithm that is using wireless link information and the architecture of a hierarchical network information. In addition S-MIP introduces a new intelligent handover mechanism [17].

The main objects which S-MIP as trying to be:

- L2 handover delay that is similar to a handover delay (in order of tens milliseconds).
- Decreasing the protocol's signaling, no more above than that for the connected hierarchical and fast approaches.
- Reduce the packet waste due to the handover delay.

A packets loss has mainly two reasons: one is the terminal packet damage occurs between the mobile node and the last access router. The other is the segment packets loss which happens between the access router and the MAP. The segment loss is due to the unpredictable nature of the handover which sometimes results on switching the data flow at the MAP while it receiving a nabbing updates, and the terminal packet damage is due to the transmission errors and the mobility. S-MIP goals to minimize both kinds of packet damages; terminal packet damage is reduced by locating the MAP as close to the mobile node as possible it's better to be located at the entry router that connects the wire network to the wireless network . Segment packets damage is reduced by using a new suggested entity called Synchronized-Packet-Simulcast (SPS). S-MIP that is using hybrid handover mechanism; the mobile node which has the highest knowledge about its present location and its accepted signal strength will begin the handover system, and then the network system will be responsible for determining the point of the following attachment. It is a decision from the movement tracking procedure, which divided the mobile node movement as one of three modes: either linearly, stationary at the middle of two overlapping access routers [18].

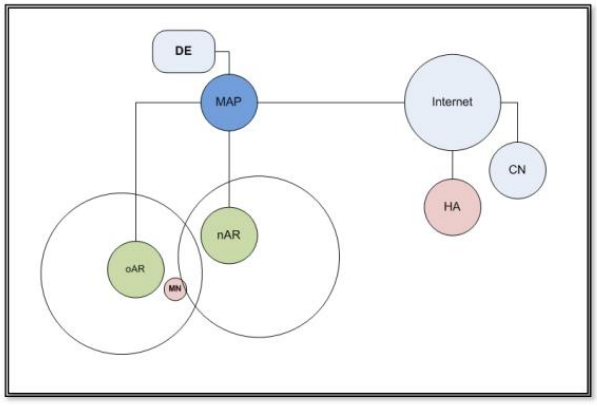

Fig. 4. Seamless MIP Architecture.

The architecture of S-MIP network is hierarchical base that is adding a new entity named decision engine (DE). Mobility Anchor Point (MAP) divides the network to domains to manage the mobility as micro or macro mobility like in hierarchical handover the Mobility Anchor Point (MAP).The decision en-

gine (DE) takes the handover decisions, and controls the handover procedure on its network domain. The DE tracking all the mobile devices in its network domain in order to identify the movement modes of the mobile nodes, and keeps a global view of the network. This will be done through periodical messages from the access routers. The DE also offers load balancing by connect the mobile node to the lower load access routers. S-MIP adds six new messages: Current Tracking Status (CTS) message from the MN to DE, which contains location tracking information. Carrying Load Status (CLS) message from the ARs to DE, which contains the information regarding how many mobile nodes an AR is currently managing. Handover Decision (HD) message from the DE to ARs, which contains the handover decision at the DE, namely which AR a MN should handover to. Handover Notification (HN) message from the OAR to MN, which contains the indication from the OAR to the MN, directing which NAR the MN should handover to. The OAR derives the content of the HN message from the received HD message. Simulcast (Scats) message from OAR to MAP. The Scats message starts the SPS process. Simulcast Off (Scoff) message from NAR to MAP. This message terminates the SPS process [19].

The Seamless handover starts when the mobile node wants to move to a new network, then it will receive beacon advertisement messages from the new entrance router, the MN will initiate the handover by sending RtSolPr message to the oAR. Then the oAR will send HI messages to all the potential nARs identified by the MN in the RtSolPr message. The HI message will contain the requested care of address on the nAR and the current care of address of the oAR. The nARs will respond by Hacks message accepting or rejecting the new care of address. In the case of the nAR accepting the new CoA, the oAR sets up a temporary tunnel to the new CoA. Or in the other case the oAR tunnels the packets to the nAR, which forwards them to the MN temporarily. Similar to the hierarchical handover the MN will receive PrRtAdv message from the oAR.

All access routers send CLS messages to the DE periodically every three seconds, which is reply to the router advertisement messages transmitted by the DE. The CLS message indicates the numbers of mobile nodes were connected to the access router and their IP addresses. The MN sends CTS message to the DE when it receives link layer beacon advertisement from a new access router. The CTS message contains information about the signal strength of the new access router. This information will be used for location tracking, ARs forward CTS every second until it receives an HD message from the DE. The DE analyzes CTS and CLS messages in order to track the mobile node movement, and then the DE tacks the decision and sends HD message to all participating ARs. Then the oAR will send HN message to the MN to indicate the next AR that the MN must handover to. According to the movement tracking the seamless handover will follow one of three procedures: The first procedure is stochastic movement mode, here the DE, using an HD message, will inform the ARs to be in anticipation mode. In this mode the mobile node will not be associated with an AR, but the AR will keep the MN's binding to be ready if the MN returning, which will reduce the unnecessary re-setup delay. The HN message from oAR to the MN indicates that the MN will switch network freely, just using fast neighbor advertisement F-NA message. The DE sends HD message to any AR if it indicates that it no longer involves requiring ending the anticipation mode. The second procedure is stationary mode; here the MN will be stationary state between two ARs coverage areas. The DE using HD message will start multiple bindings between the MN and the ARs, which enable the MN to use more than one CoA at the same time. The third procedure is linearly movement mode; here the HD message contains the AR to which the MN wills handover to. Another HD message will be sent to the rest of the ARs that are not selected by the DE.

Then the MN will just need to send F-BU message to the oAR after it receives the HN message and form the new CoA, in order to bind its present on link address to the new CoA. Then the oAR will send the Scast message to the MAP to initiate the simulcasting of the packets, which mean the duplication and sending the packets to both the oAR and the nAR at the same time. The oAR will send the F-Back message to both the current and the new networks to ensure that the MN receives its message. After receiving the F-NA message the nAR starts forwards packets to the MN, at the time the oAR is also forwarding packets to the nAR, and sending all the packets on the wireless channel to ensure the reception by the MN in case it does not switch networks immediately. Then nAR will send Soff message to the MAP after it forwards all the packets transmitted by the oAR to the MN. The MAP then updates binding of the new on link address of the MN with its regional CoA. The Soff message will be forwarded to the DE, which will not permit the mobile node to execute another seamless handover before the current one is completed. Some modifications to the standard router advertisement message must be done. Similar to hierarchical handover the MAP discovery option added to the router advertisement message enabling the MN to discover the MAP. The DE reply option also must be added to the router advertisement, in order to synchronize the timing of the CLS message from ARs to the DE. This synchronization of CLS messages in addition to the periodic CTS messages is important to the calculation of the movement tracking and also to the handover algorithm.

3.5 MIFA Description

For the initial registration, the MN uses the regular MIP procedures. In addition, the MN informs the FA and the HA that it prefers to use MIFA in future registrations [20]. As a response to this, the HA builds a security association between the HA and the FA-K1FA-HA on one side and between the MN and the FA on the other side K1MN-FA. The FA in turn derives the keys, generates two random variables R1, R2, generates another key (K2MN-FA) between the MN and the FAs in the L3-FHR, to which the present FA associated to, encrypts K2 MN-FA with K1 MN-FA, add R1, R2 and the encrypted K2 MN-FA in extensions to the Reg-Rply message, authenticates the new message with K1 MN-FA, and sends it to the MN. Next, the FA performs the Initial_Authentication_ Exchange procedure.

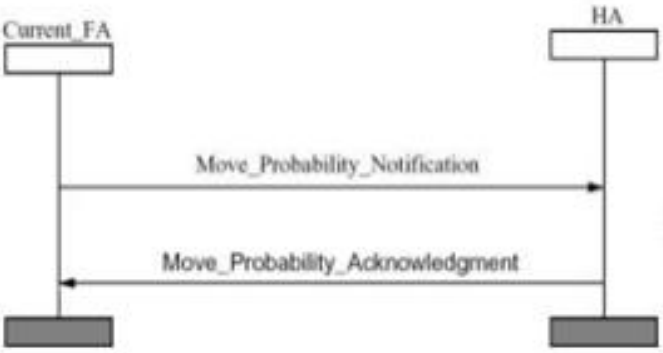

Fig. 5. Initial_Authentication_Exchange.

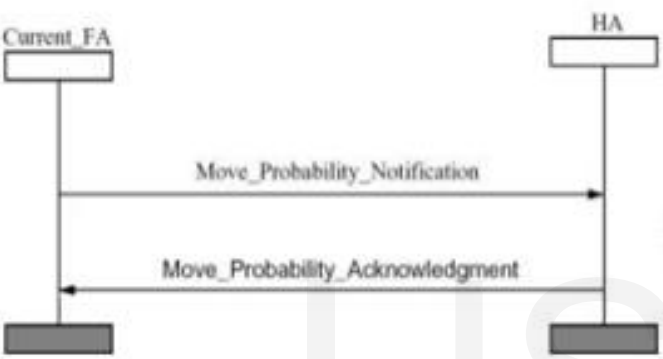

Fig. 6. Move_Notification.

With this procedure, the current FA sends a Move_Probability_Notification to the HA. The message contains two random variables R1, R2 and the security association between the HA and whole FAs in the L3-FHR, to which the current FA belongs to, (K2 FA-HA). This key is encrypted with K1 FA-HA, which has been generated during the initial registration. K1 FA HA authenticates this message too. The HA responds to the notification by sending an Acknowledgement (Move_Probability_Acknowledgement).

In order to notify the FAs in the neighbourhood of a potential handoff of a MN, the current FA performs the Move_Notification procedure (Figure 6). With this procedure the current FA transmits a Move_Probability_Notification to all of the FAs in the L3-FHR. The message contains the security organizations between the MN and the FAs in the L3-FHR (K2 MN-FA) and between these FAs and the HA (K2 FA-HA). These security associations are encrypted with the shared security organization existing between the FAs (K FA-FA), which authenticates these messages too. The MN will move to one of these FAs. As a result, the two keys will be used by one of these FAs and deleted from the others, when the keys lifetime expires. Each neighbouring FA replies optionally a Move_Probability_ Acknowledgment as a response to the notification, as depicted in figure 6.

Next, the Authenticators_Exchange procedure is executed as shown in figure 6 to transmit the authentication information to every FA of the L3-FHR. Each FA in the L3-FHR sends an Authentication_Information_Request to the HA. This message is authenticated by K2 FA-HA. The HA then responds by an Authentication_Information_Response. This message contains the authentication values that the MN and the HA have to produce in the next registration. In addition, the message includes the supported features of the HA (e.g. simultaneous binding, GRE, etc.) which are required by the FA to decide whether the MN is authenticated or not and whether the requirements of the MN can be satisfied or not. These features are used to support replay protection too. This message is authenticated by K2 FA-HA. The Authenticators_Exchange procedure is optional as depicted in figure 7. Instead of using this procedure, the information existing in the Authentication_Information_Response can be sent with the Move_Probability_ Acknowledgment message sent from the HA to the current FA during the Initial_Authentication_ Exchange procedure. The current FA spreads this information to the neighbouring FAs with Move_Probability_Notification procedure. This guarantees the scalability of MIFA [20].

When the MN moves to one of these FAs it performs the Registration_by_Neighbour _Agent procedure (Figure 8). The MN gets an Agent_Advertisement, which indicates that the current FA supports MIFA. The MN builds and sends a Reg_Rqst to this FA. This message includes MIFA authentication information and will be authenticated by the security association existing between the MN and the FA (K2 MN-FA). The current FA then compares the MN-FA authentication information using K2 MN-FA. If the authentication succeeds, it compares the MIFA authentication information and the identification field, to be sure that the replay protection requirements are met. If these requirements are met, the current FA examines whether the HA can satisfy the requirements of the MN (by examination of the features supported by the HA). If this examination is successful, the current FA sends a Previous_FA_Notification to notify the previous FA that it must tunnel the packets destined to the MN, to the current FA. This message is authenticated by the FA-FA security association (K FA-FA).

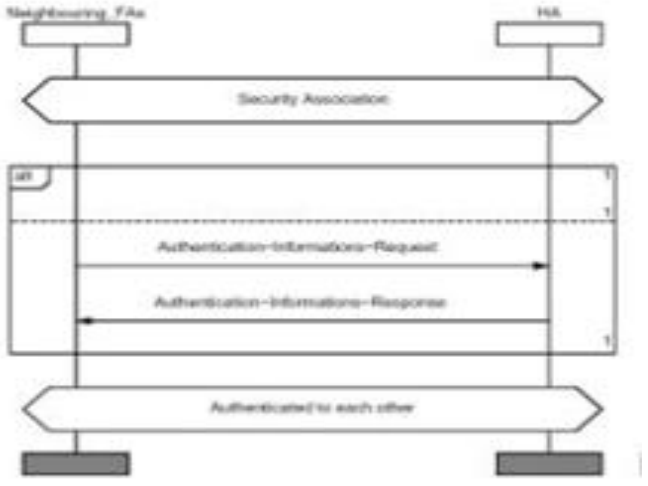

Fig. 7. Authentication_Exchange.

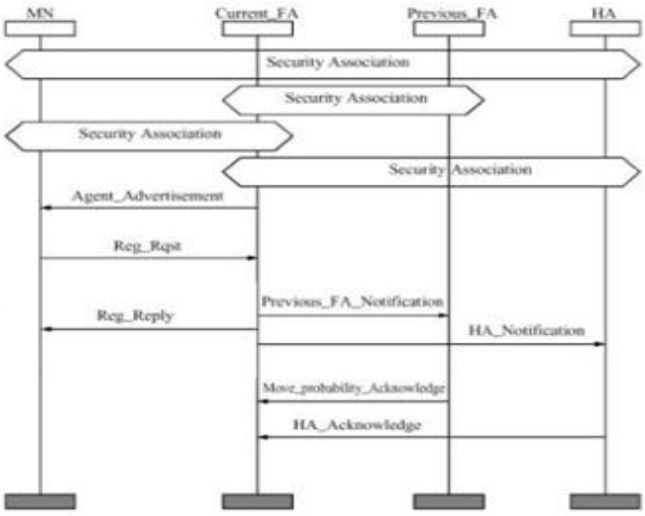

Fig. 8. Registration_by_Neighbour_Agent.

The current FA then generates two random variables R1, R2, generates the keys (K3FA-HA , K3 MN-FA), which will be used to authenticate the messages in the next registration with the next FA in the L3-FHR, encrypts K3MN-FA with K2MN-FA and sends Reg-Rply message to the MN. This message contains of extensions containing R1, R2, and the encrypted K3MN-FA additionally to the standard fields used by MIP. After that the current FA encrypts K3FA-HA with K2FA-HA and sends an HA_Notification to notice the HA about the recent binding, the two random variables and the encrypted K3FA-HA are sent with this message. The HA then sends an HA_Acknowledgment message and starts to establish the tunnel to the current FA. The HA_Acknowledgment message covers the information existing in Authentication_ Information_Response message if the Authenticators_Exchange procedure is not in use. After that the current FA starts then the Move_Notification procedure. When the previous FA receives Previous_FA_Notification message it sends a Move_Probability_ Acknowledgment as a response to this message and starts the tunneling of the packets destined to the MN to the new FA.

In order to be compatible with MIP and to avoid that the communication is disrupted due to a loss of a MIFA control message, each MIFA Registration Request has to contain the MN-HA authentication augmentation. When a failure happens during any MIFA procedure (message loss), the Reg_Rqst will still be processed by MIP [21].

4 Comparison & Analysis

4.1 Comparison between MIFA & Mobile IP

We have planned a simple analytical sampling or model to balance the raised protocol with Mobile IP. The network topology applied is exhibited in Figure 10. We prescribe the following words:

T WL: Time needed for a message to pass via the wireless link from the MN to the FA.

T W: Time needed for a message to pass via the wired link from the FA to the HA.

T PFA: Time needed for a message to pass via the wired link from the present FA to the prior FA.

P MN: Time needed by the MN to move or process the registration.

P FA: Time needed by the FA to process the registration.

P HA: Time needed by the HA to process the registration.

P PFA: Time needed by the preceding FA to process the registration.

We prescribe the following values: TWL= 5 ms, TW = 10 … 100 ms, TPFA = 5 ms. The processing time for the function of hash for authentication (HMAC-MD5) [22] is assumed to be 1 ms. The assumed time to create a key and to construct a message is 1 ms, respectively. The estimation starts from the time of geeting an Agent_Advertisement message from the FA. The security associations (SA) disscussed in this experiment in the case of MIFA are: MN-current FA_SA, current FA-HA_SA, current FA-previous FA_SA and MN-HA_SA. In the case of MIP MN-HA_SA is disscussed.

In the case of MIP, the time needed by the MN to restart transmission in uplink and to get data in downlink is provided by equation [1]:

TMN-Uplink = TMN-Downlink = TMN = P + 2*T [1]

Where T = TWL + TW and P = P MN + PFA + PHA

Filling in the values marked above, we got the equation [2]:

TMN (ms) = 25 + 2 * T W [2]

From the equation [2] we inform, that the time TMN dependents on TW. Thus, this time will increase when TW rises. In the MIFA case, the time needed to restart transmission in uplink by the MN is independent of TW and given by equation [3]:

TMN-Uplink=P+2*T [3]

with T = TWL and P = PMN + PFA

Entering the accepted values, we got the equation [4]:

TMN-Uplink (ms) = 40ms [4]

From equation [4] we inform, that the time TMN-Uplink is independent of TW. Thus, an increase of TW does not have a negative influence on the operation of MIFA. The time needed to restart reception of downlink data is provided by equation [5]:

TMN-Downlink=P+2*T [5]

Where P = PMN + PFA + PPrevious FA and T = TWL + TPFA

Entering the assumed values, we got equation [6]:

TMN (ms) = 50ms [6]

The calculations display that MIFA benefits from the installed tunnel among the HA and the previous FA. Until the

new tunnel among HA and present FA is installed, MIFA uses an additional tunnel from the previous FA to the present FA. Thus, the time needed for the MN to resume reception of data in downlink is distinct of TW as well. This means that MIFA performs a seamless and fast handoff free of TW, i.e. the distance between FA and HA. Until a new tunnel among the HA and the present FA is installed. The preceding FA forwards packets to the present FA. Thus, the latency resulting from the establishment of the new tunnel among current FA and HA is hidden [22].

Figure 9 shows the time needed to restart transmission in uplink by the MN for MIFA and MIP when TW= 10, 25, 50, 75 and 100 ms, respectively. From the figure we can be noticed that MIFA is faster than MIP even when the HA is near to the FA. E.g. for TW= 10 ms, MIFA is 5 ms faster than MIP. When TW improves, the advantage of MIFA increases. The time needed in case of MIP is dependent on TW and will increase when TW increases. However, in the case of MIFA this time is independent of TW. Therefore, it will not rise (TW= 25 ms, MIFA is 35 ms faster than MIP; TW= 50 ms, MIFA is 85 ms faster than MIP; TW= 75 ms, MIFA is 135 ms faster than MIP).

In Figure 10, the time needed to resume data reception in downlink by the MN is displayed for MIFA and MIP when TW= 10, 25, 50, 75, and 100 ms, respectively. The figure depicts that MIP is(1 to 5 ms) faster than MIFA when the HA is near to the FA (TW= 10 to 12 ms). However, if TW increases, MIFA will outperform MIP.

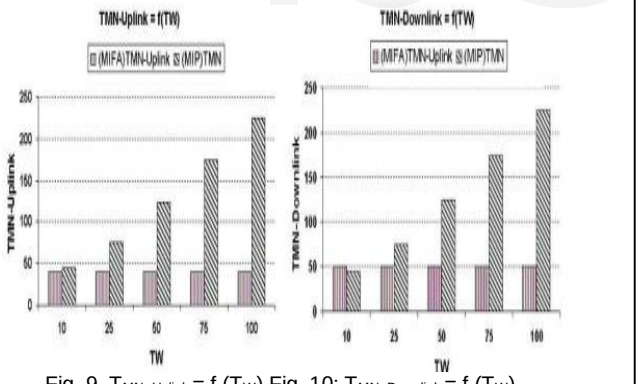

Fig. 9. $T_{MN\text{- }Uplink} = f(T_W)$ Fig. 10: $T_{MN\text{- }Downlink} = f(T_W)$.

For this case the independence of MIFA from the distance between the HA and the FA makes it faster than MIP (T W = 25 ms, MIFA is 25 ms faster than MIP; TW= 50 ms, MIFA is 75 ms faster than MIP; TW= 75 ms, MIFA is 125 ms faster than MIP).

We summarize that because of the independence of MIFA from TW, it is more efficient than MIP for most cases, especially where the time needed for the message to pass via the wired link between the present FA and the HA is large. Additionally, MIFA eliminates the reasons for latency present in MIP. Moreover, MIFA increases the security of the connection due to the mandatory addition of the FA in the security association.

4.2 Comparison between MIFA and Hierarchical Mobile IP

In order to assimilation MIFA with Hierarchical Mobile IP (HMIP) another simple analytical model has been planned [23]. The network topology used for this study is shown in Figure 10. We define the following terms:

T1, T2, T3: The time needed for the message to running through two adjoining nodes on the wired link.

PRFA : The processing time needed by the provincialism FA for the registration.

PGFA : The processing time needed by the GFA for the registration.

The following values for these terms are assumed: T1 =T2 =T3 = 3 ms, TWL = 3 ms, TPFA = 3 ms and TW = 10…100 ms. The calculation starts from the time of receiving an Agent_Notification message from the new FA.

When we suppose that the MN initially records with the FA1 (see Figure 10) the details in equation [1] will be:

T = TWL + TW + T1 + T2 + T3 and P = PMN + PFA1 + PRFA3 + PRFA1+ PGFA+ P HA

When we enter the values individualize above, we obtain equation [7]:

THMIP-Uplink=THMIP-Downlink=49,5+2*TW [7]

Thus, the disruption time will improve when TW increases. In the case of MIFA, the time after which the MN can resume transmission in uplink is given by equation [3] with the terms T = TWL and P = PMN + PFA1

Applying the assumed values, we get:

TMN-Uplink (ms) = 27ms [8]

The time needed to restart felicitation in downlink is given by equation [5] with the terms:

T = TWL and P = PMN + PFA1 + PPFA

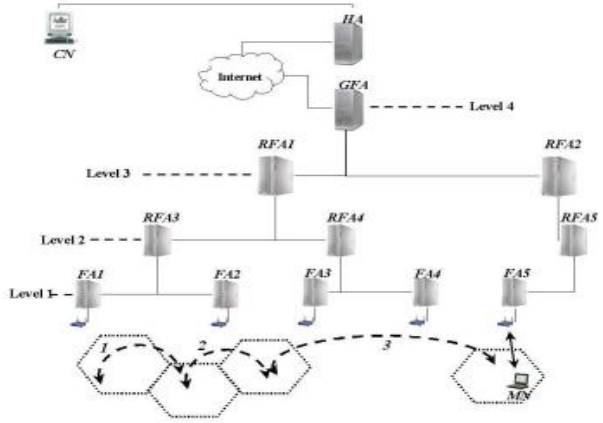

Fig. 10. Network Topology for HMIP.

Filling in the assumed values we get

TMN-Downlink (ms) = 39ms [9]

Figure 11 shows the relation between TMN-Downlink and TMN-Uplink for TW = 10, 25, 50, and 100 ms, respectively. In Figure 5.4 we see that for the case that the MN enters a new domain,

This is similar to MIFA. In case the MN moves from the area included by the FA1 to the area included by the FA2, only the RFA3 must be aware of this movement. This means that the MN registers with the second level of the hierarchy. The time needed by HMIP for the registration with RFA3 is defined again by the equation [1] with the terms:

T = TWL + T1 and P = PMN + P FA2 +P RFA3

Entering the assumed values specified above, we get:

THMIP-Uplink=THMIP-Downlink=24ms [10]

we obtain the time required to complete the registration with RFA1 for the case that the MN supports HMIP. P and T are defined as follows:

T = TWL + T1 + T2 and P = PMN + PFA3 + P RFA4 + PRFA1.

Entering the assumed values, we get:

THMIP-Uplink=THMIP-Downlink=32ms [11]

This means that the MN registers with the fourth level of the hierarchy. The time required in case of HMIP to complete the registration with the GFA is given by equation [1], too. P and T are defined as the follows:

T = TWL + T 1 + T 2 + T3 and P = PMN + PFA5 + PRFA5 + PRFA2 + PGFA

Filling in the values as specified above, we get:

THMIP-Uplink=THMIP-Downlink=40ms [12]

Figure 12 shows a comparison between the time required to resume transmission in uplink and to continue receiving in downlink in the case of MIFA and in the case of HMIP, Figure12 shows that HMIP outperforms MIFA in the case that the second level of the hierarchy is informed about the movement of the MN. In opposite to this, the MN resumes transmission in uplink 5 ms earlier with MIFA. If the movement is controlled by the fourth level of the hierarchy, MIFA is faster than HMIP in the both directions. The MN resumes reception in downlink 1 ms faster with MIFA than with HMIP. In uplink the advantage of MIFA is 13 ms. these differences remain constant regardless of TW [20].

Summarizing the comparison, we can state the following:

- MIFA adds extra security to the connection because the FA authenticates the MN by using the MN-HA and the MN-FA security association while HMIP authenticates the MN only by using the MN-FA security association.
- With respect to performance, MIFA and HMIP are comparable.
- MIFA may be combined with HMIP to improve the handoff between the domains. This can be achieved by supporting MIFA in the GFAs.

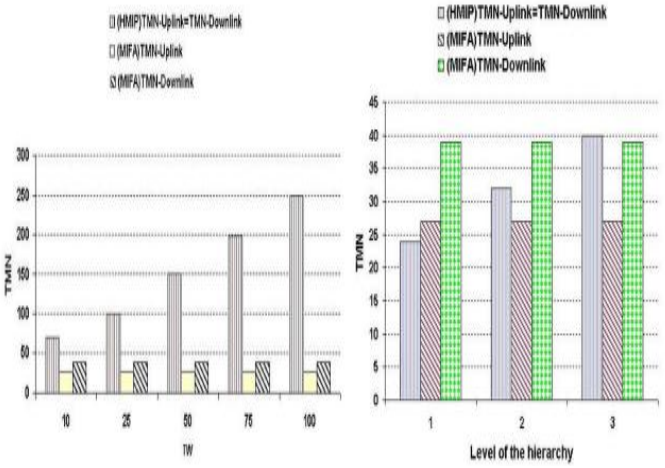

Fig. 11. $T_{MN\text{-}Downlink\ /\ -Uplink} = f(T_W)$ and Fig. 12. Comparison Between MIFA and HMIP for the different Hierarchical Levels.

4.3 Comparison between MIFA and Seamless Mobile IP

The handover delay, packet loss and bandwidth for MIP and S-MIP is compared and seen that S-MIP is a better approach than MIP [24].

Handover Delay:

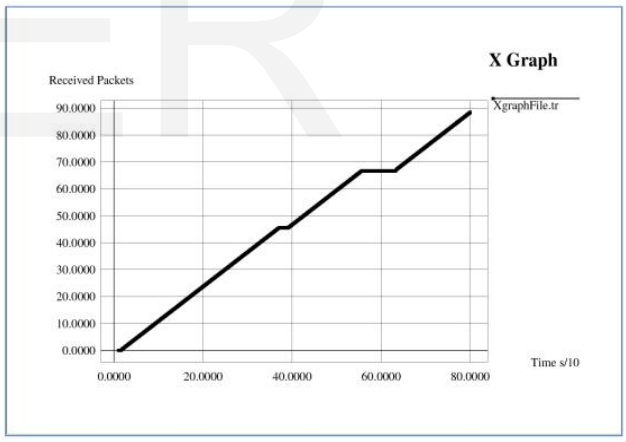

Fig. 13. Handover Delay for Standard MIP.

Figure 13 shows the handover delay for the standard mobile IP, the black line represents the received packets which indicate the mobile node's (MN) receiving buffer contents. The correspondent node (CN) transmits UDP packets to the mobile node (MN); the line shows the end to end UDP connection versus the simulation time.

From the figure we can notice there were two handover processes during the simulation time: one at t = 37 and the other at t = 55. The first handover happened when the MN moved from the HA to the oAR, and the second handover was happened when the MN moved from the oAR to the nAR

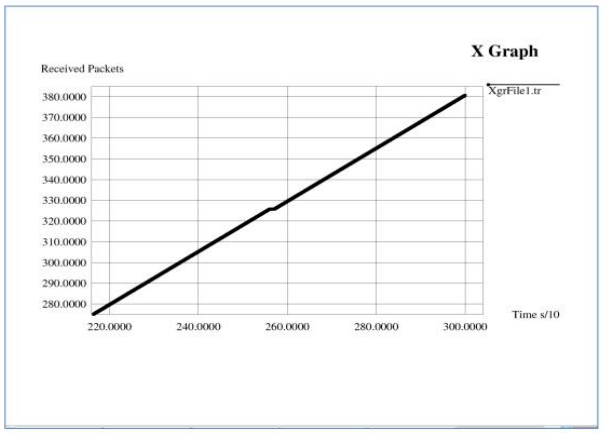

Fig. 14. Handover Delay for Seamless Mobile IP.

Figure 14 shows the handover delay for the seamless mobile IP, the black line represents the received packets which indicate the contents of the mobile node's (MN) receiving buffer. The correspondent node (CN) transmits UDP packets to the mobile node (MN); the line shows the end to end UDP connection.

From the figure we can notice there was one handover process took place during the simulation time at t = 255. The handover was happened when the MN moved from the oAR to the nAR. The handover delay of the S-MIP case was shorter compare to the standard MIP case (figure 13).

Bandwidth:

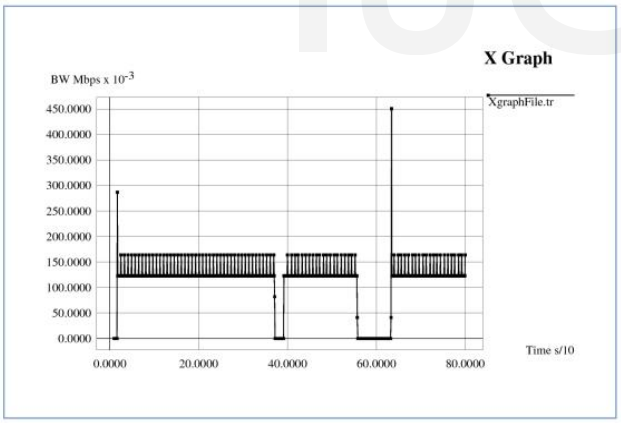

Fig. 15. Link Usage for Standard MIP.

Figure 15 shows the link bandwidth in megabit per seconds for the standard mobile IP, the black line represents the bandwidth of the received packets which indicates the mobile node's (MN) receiving buffer contents. The correspondent node (CN) transmits UDP packets to the mobile node MN, the line shows the end to end UDP connection.

From the figure we can notice there were two handover processes during the simulation time: one at t = 37 and the other at t = 55. The range of the link bandwidth was been about 0.125 and 0.16 Mbps. During the handover processes the link bandwidth was reached to zero, which means there were no received packets by the MN at that time.

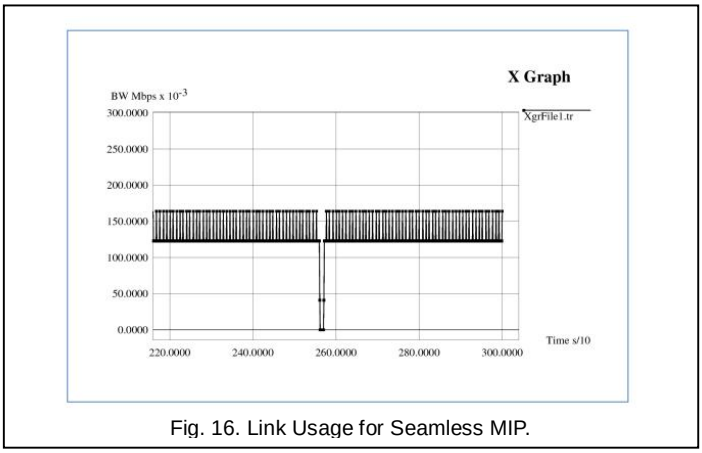

Fig. 16. Link Usage for Seamless MIP.

Figure 16 shows the link bandwidth in megabit per seconds for the seamless mobile IP, the black line represents the bandwidth of the received packets which indicates the contents of the mobile node's (MN) receiving buffer. The correspondent node (CN) transmits UDP packets to the mobile node (MN); the line shows the end to end UDP connection.

From the figure we can notice the handover process during the simulation time: one at t = 255. The range of the link bandwidth was been about 0.125 to 0.16 Mbps the same like in the MIP case. During the handover processes the link bandwidth reached zero, which means there were no received packets by the MN at that time. The amount of the lost bandwidth is reduced by the S-MIP in this case compared to the standard MIP case, and as well the link usage is also being better.

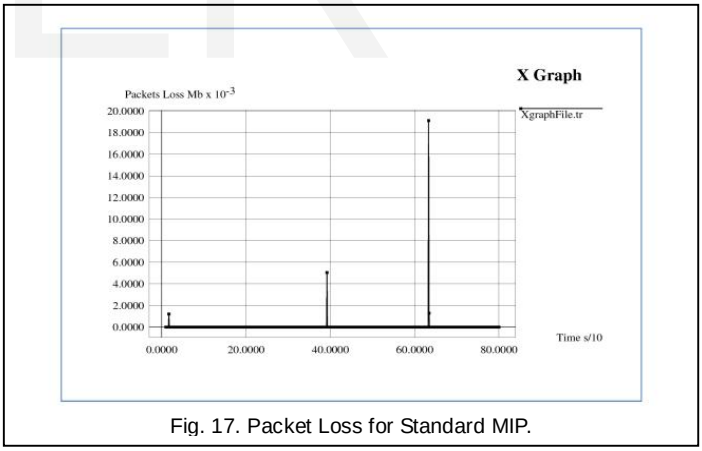

Fig. 17. Packet Loss for Standard MIP.

Figure 17 shows the packets loss in megabytes for the standard mobile IP; the black line represents the amount of the lost packets from the received packets.

From the figure we can notice there were three points for the packets loss during the simulation time: one at t = 3, t = 38 and the other at t = 55. The lost packets at the first point caused by the first sending of the packets and no handover was involved, it is about 0.00125 Mb. The second point caused by the first handover process and it reach to 0.005Mb, and the last point is also caused by the second handover process and the packets loss reach to 0.018 Mb.

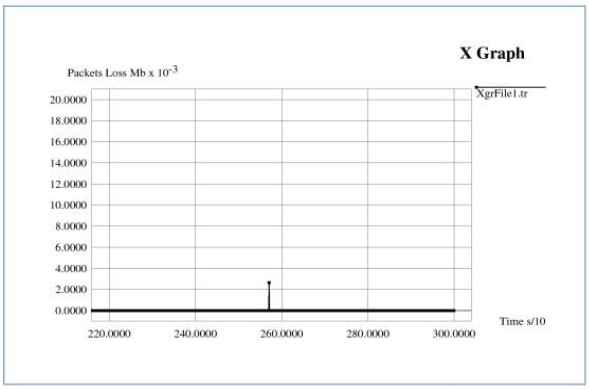

Fig. 18. Packet Loss for Seamless MIP.

Figure 18 shows the packets loss in megabytes for the seamless mobile IP; the black line represents the amount of the lost packets from the whole received packets.

From the figure we can notice there was one point for the packets loss during the simulation time: at t = 255. The packet loss at this point caused by the first handover process and it reach to 0.00275Mb, and it's less than the value of the lost packets for the standard MIP case.

4.4 Comparison and Result

We saw that, MIFA performs a seamless and fast handoff independent of TW, i.e. the distance between FA and HA. MIFA is faster than MIP even when the HA is close to the FA. E.g. for TW= 10 ms, MIFA is 5 ms faster than MIP. For this case the independence of MIFA from the distance between the HA and the FA makes it faster than MIP (T W = 25 ms, MIFA is 25 ms faster than MIP; TW= 50 ms, MIFA is 75 ms faster than MIP; TW= 75 ms, MIFA is 125 ms faster than MIP).

MIFA is more efficient than HMIP for the both directions (uplink and downlink). This is because of the independence of MIFA from TW. MIFA in the case that the second level of the hierarchy is about 3 ms faster than MIFA in uplink and about 15 ms faster in downlink. In opposite to this, the MN resumes transmission in uplink 5 ms earlier with MIFA. MIFA is faster than HMIP in the both directions.

The handover delay of the S-MIP case was shorter compare to the standard MIP. From the figure we can notice there were three points for the packets loss during the simulation time: one at t = 3, t = 38 and the other at t = 55. The lost packets at the first point caused by the first sending of the packets and no handover was involved, it is about 0.00125 Mb. The second point caused by the first handover process and it reach to 0.005Mb, and the last point is also caused by the second handover process and the packets loss reach to 0.018 Mb. And there was one point for the packets loss during the simulation time: at t = 255.

5 Conclusion

The analytical calculation shown by Khalid Eltayb Aldalaty mentioned that the handover delay for standard mobile IP is 416 ms and for seamless mobile IP is 144 ms which is shorter than standard mobile IP. So, seamless MIP is a better approach than standard MIP.

In comparison together with MIP, MIFA abates the re-access secrecy, and seize the FA to access the MN purely [24]. Thus, there is no diminution of security. This may abates the puzzle with wireless TCP bracing. Assimilation with HMIP displays that MIFA is analogous to HMIP with regard to performance and does not needed the hierarchic formation of mobility-aware tumor the paradigm with HMIP. In connection, MIFA can associated together HMIP to increase the handoff between the domains. If we could combine the MIFA and S-MIP, then the real time application could be possible.

References

[1] C. Janey and C. Hoe, "Improving the start-up behavior of a congestion control scheme for TCP," *Proc. Int. Conf. on Applications, technologies, architectures, and protocols for computer communications*, California, USA, pp. 270-280, Aug. 1996.

[2] Nazmul Hossain and Md. Alam Hossain, "Integrated Cellular and Ad Hoc Relaying Systems: Analysis of Call Blocking Probability & Performance," International Journal of Scientific & Engineering Research (IJSER), vol. 6, no. 12, pp 635-643, Dec. 2015.

[3] J.O. Vatn, "Improving Mobile IP handover performance," Licentiate thesis, ISRN KTH/IT/AVH--00/06-SE, Department of Teleinformatics, Royal Institute of Technology, Stockholm, Sweden, Jun. 2002.

[4] H. Andersson, S. Josefsson, G. Zorn, and B. Aboba, "Protected Extensible Authentication Protocol", Internet Draft October 2001, http://tools.ietf.org/html/draft-josefsson-pppext-eap-tls-eap-01.txt.

[5] Chiussi F., Khotimsky A., Krishnan S. (2002). "Mobility Management in Third-generation all-IP networks". IEEE Communications Magazine 40(9): 124–135

[6] C. Perkins "IP Mobility Support for IPv4," RFC 3344, Aug. 2002.

[7] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6", RFC 3775, Jun. 2004.

[8] D. Le, X. Fu, and D. Hogrefe, "A Review of Mobility Support Paradigms for the Internet," IEEE Communications Magazine, vol. 8, no. 1, pp. 120-126, Apr. 2006.

[9] E. Hernandez and A. Helal, "Examining Mobile IP Performance in Rapidly Mobile Environments: The Case of a Commuter Train", *in Proc. of 26th IEEE Local Computer Networks (LCN'01)*, FL, 2001, pp. 365–372.

[10] "Wireless Communications and Networks", William Stallings, Fourth Edition, Nov. 2004.

[11] C. Perkins "Mobility Support in IPv6," RFC 6275, Jul. 2011.

[12] C. Pignataro "IPv6 Support for Generic Routing Encapsulation (GRE)," RFC 7676, Oct. 2015.

[13] G.P. Pollini, "Trends in handover design," *Proc. IEEE Communications Magazine*, vol. 34(3), pp. 82 - 90, Aug. 2002. doi: 10.1109/35.486807

[14] G. Chellani, and A. Kalla, "A REVIEW: STUDY OF HANDOVER PERFORMANCE IN MOBILE IP," International Journal of Computer Networks & Communications (IJCNC), vol. 5, no. 6, pp 137- 151, Nov. 2013.

[15] V. Vassiliou, and A. Pitsillides, "Supporting mobility Events within a Hierarchical Mobile IP-over-MPLS Network," Journal of Communications, vol. 2, no. 2, pp. 61-70, Mar. 2007.

[16] Y. Gvvon, J. Kempf and A. Yegin, "Scalability and robustness analysis of mobile IPv6, fast mobile IPv6, hierarchical mobile IPv6, and hybrid IPv6 mobility protocols using a large-scale simulation," *Proc. Int. Conf. on communications,* Paris, France, Jul. 2004. doi: 10.1109/ICC.2004.1313318

[17] Perkins C. "Mobile Networking through Mobile IP". IEEE Internet Computing, 2(1), pp. 58–69, 1998.

[18] I. W. Wu, W. S. Chen and H. E. Liao, "A seamless handoff approach of Mobile IP protocol for mobile wireless data networks," IEEE Transactions on Consumer Electronics, vol. 48, no. 2, pp 335 - 344, Aug. 2002, doi: 10.1109/TCE.2002.1010140

[19] R. Hsieh, Z. G. Zhou and A. Seneviratne, "S-MIP: A Seamless Handoff Architecture for Mobile IP," *Proc. INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications*. IEEE Societies, San Francisco, USA, pp. 1774-1784, Apr. 2003, doi: 10.1109/INFCOM.2003.1209200.

[20] A. Diab, A. Mitschele-Thiel and R. Boringer, "Evaluation of Mobile IP fast authentication protocol compared to hierarchical mobile IP," *Proc. in IEEE International Conference on Wireless And Mobile Computing, Networking And Communications*. IEEE Societies, Montreal, Canada, Aug. 2005, doi: 10.1109/WIMOB.2005.1512844

[21] A. Diab, A. Mitschele-Thiel and J. Xu, "Performance analysis of the mobile IP fast authentication protocol," *Proc. of the 7th International Symposium on Modeling Analysis and Simulation of Wireless and Mobile Systems (MSWiM 2004)*, Venice, Italy, Oct. 2004, doi: 10.1145/1023663.1023715

[22] R. Hsieh, and A. Seneviratne, "A Comparison of Mechanisms for Improving Mobile IP Handoff Latency for End-to-End TCP," *Proc. MobiCom'03 IEEE Global Telecommunications Conference*, San Diego, California, USA, vol. 3, pp. 2488 - 2492, Sep. 2003, doi: 10.1109/GLOCOM.2002.1189078.

[23] R. Hsieh, and A. Seneviratne, "Performance analysis on Hierarchical Mobile IPv6 with Fast-handoff over End-to-End TCP," *Proc. GLOBECOM IEEE Global Telecommunications Conference*, Taipei, Taiwan, vol. 3, pp. 2488 - 2492, Nov. 2002, doi: 10.1109/GLOCOM.2002.1189078.

[24] X. C. Pérez, M. T. Moreno and H. Hartenstein, "A performance comparison of Mobile IPv6, Hierarchical Mobile IPv6, fast handovers for Mobile IPv6 and their combination," ACM SIGMOBILE Mobile Computing and Communications, vol. 7, no. 4, pp. 5-19, Oct. 2003, doi: 10.1145/965732.965736