PERFORMANCE ANALYSIS OF A SECURE SEAMLESS HANDOVER MECHANISM IN ALL-IP NETWORKS

Alf Zugenmaier, Anand Prasad, Julien Laganier

DoCoMo Euro-Labs

lastname@docomolab-euro.com

Landsberger Straße 312

80687 München

Germany

Phone: +49 89 56824 0

ABSTRACT

Beyond third generation or B3G is the next generation of mobile networks that will comprise a heterogeneity of radio access technologies with a common IP core. Support for terminal mobility and thus handover is a key feature of these networks.

Handover occurs when a terminal changes its point of attachment from one access router to another. Communication is not possible during the change in point of attachment. To ensure service continuity it is necessary to keep this interruption as short as possible.

This paper quantitatively evaluates the performance of a secure proxy mobility protocol (ProMPt) that supports fast mobility between heterogeneous access networks in one operator's domain. ProMPt is designed by integrating access security and mobility support for optimal performance instead of layering protocols for these two purposes. To enable quantitative evaluation, a test bed was setup with realistic wireless link emulation and an implementation of a basic ProMPt state machine. Results show that ProMPt outperforms Mobile IPv6 combined with EAP-AKA by one order of magnitude thus providing better service when a terminal moves between different access routers.

KEY WORDS

Communications / Network Security, Mobile Computing Security, Handover Performance

PERFORMANCE ANALYSIS OF A SECURE SEAMLESS HANDOVER MECHANISM IN ALL-IP NETWORKS

1 INTRODUCTION

Beyond third generation (B3G) networks as envisioned today will try to take advantage of the manageability and predictability of third generation (3G) mobile cellular networks combined with the ease of deployment of higher data rate wireless LAN (WLAN) technologies. Research and standardization activities are on-going towards development of a new air interface and towards development of solutions for integration and interworking between different access technologies. While this task seems easy – both 3G networks and WLANs support IP packet data – much work is needed to provide seamless mobility such that the user does not notice handovers while at the same time maintaining the network's and user's security.

One important concept in 3G networks is that of the home operator. The home operator has a contract with the subscriber, which allows billing for services used. The home operator also operates the authentication server. It has all information necessary to identify the subscriber or rather, the subscriber's equipment called the mobile node for the remainder of this paper.

Usually a home operator provides network services in a region or country. Roaming contracts between home operator and foreign operators allow subscribers to make use of services in regions not covered by the home operator.

Thus, the mobility that is supported by mobile networks is fourfold: the air interface supports mobility of a mobile node within an access point's coverage region. Mobility of the node between access points is supported, i.e. handover from one access point to another. This is also the case for access points of differing technologies such as wireless LAN and cellular networks. Movement can take place between networks of different operators.

The problem is how to achieve fast handovers for roaming subscribers, i.e., subscribers not attached to their home network, but within the coverage area of one foreign operator. The special problems arising in this scenario come from the fact that the home network and thus the authentication server of the subscriber may be far away, leading to a potentially large delay if entities in the home network have to be contacted.

Functional requirements for a solution are:

- Handovers should happen in less then 50ms, as this is an acceptable buffering delay and fits well in ITU-T[1] recommended one way delay for real-time voice and video traffic over IP.
- The network should be able to control routing of traffic.
- The solution should not interfere with other mobility management schemes the mobile node wishes to employ.

Security requirements are:

- For network access security, the same authentication database should be used for authenticating subscribers to 3G networks and wireless LANs.

---

[1]ITU-T is the telecommunication standardization sector of the International Telecommunications Union (ITU) within the United Nations System

- Location privacy should be given for a mobile node with respect to its correspondent nodes, i.e. no information about the location of the mobile node should be visible to anyone communicating with it.

The conventional approach to developing a solution to this would be to design the mobility mechanism first and security on top of it. The performance of these approaches is not sufficient to achieve the goal of seamless handovers. However, even when co-designing the mobility support and the security solution, the performance goal is ambitious.

The contribution of this paper is to present performance measurements of a simulation for ProMPt, a solution that was designed by the authors of this paper. These measurements give an indication as to how ProMPt can be improved

The paper is structured as follows: First we review existing literature with respect to performance analysis and determine the state of the art of potential solutions. Then we review one secure mobility management solution in Section Three and show its operation. Section Four describes the simulation setup. The results of the simulations are presented and discussed in Section Five. Conclusions and Outlook finalize the paper.

2 RELATED WORK

There are a number of mobility mechanisms that provide IP layer continuity for mobile users. Mobile IP has been standardized for both IPv4 [1] and IPv6 [2]. Central to both mobile IP solutions is the home agent. This is a process on a node, usually a router. The home agent assumes the IP address of the moving node while the mobile node is off the home link which is the link having the same prefix as the home address of the mobile node. The home agent acts as proxy forwarding traffic to the current address of the mobile node. IPv6 includes route optimization, which allows to avoid this triangular routing. The performance of this solution is not sufficient because movement of the mobile node is always indicated to the home agent, which, for roaming users, may be on the other side of the world. For mobile IPv6 optimizations exist.

Fast mobile IP (FMIP) [3] is an optimization to allow a mobile node to pre-configure itself for its next location. It also offers support for redirection of packets that are already destined for the old address of the mobile node.

Hierarchical mobile IPv6 (HMIPv6) [4] introduces a local mobility anchor point, which in this case is basically a hierarchy of home agents. This architecture of this solution is very similar to our proposal. However, HMIPv6 requires every node that wishes to take advantage of fast handovers to be HMIPv6 aware. In addition, the network cannot decide how to allocate resources, all handovers are controlled by the mobile node. These two issues are addressed by ProMPt. In fact, ProMPt proxies HMIPv6 with access routers taking over mobility management.

Non-IETF approaches include cellular IP [5], HAWAII [6], and BRAIN BCMP [7].

The basic concept of cellular IP is similar to that of Ethernet switching. Every router maintains a database of on which port packets with a particular source IP address are received. This is an indication that this IP addressed can be reached by forwarding packets destined to this address via the port stored in the database. This approach only works if the uplink and downlink paths of data packets are identical.

In HAWAII[2] the network is segregated into domains served by one root router. The mobile node sets up a tunnel to the root router responsible for the domain it is in. All communication with the mobile node is via this router. A macro mobility solution such as mobile IP deals with mobility

[2] Not the island, the mobility support solution

between domains. The micro mobility employed within a domain is based on actively maintaining a routing path between the root router and the mobile node.

Similarly, BRAIN BCMP separates various access network domains. It is based on a meshed topology of the access network, which is in contrast to HAWAII, cellular IP, and the IETF approaches that base on routing trees.

All of the above solutions have in common that access control to the access network is seen as an orthogonal problem.

Access control is usually based on authentication. Authentication in 3G networks uses the authentication and key agreement protocol (see e.g. [8]). Authentication in wireless networks employs the extensible authentication protocol EAP [9]. The EAP protocol serves as a base protocol to transport authentication messages between the mobile node and an authentication server. Various authentication protocols have been defined, including RADIUS over EAP [10], TLS over EAP [11], and AKA over EAP [12].

The usual way of dealing with handover procedures in wireless LANs is to layer the mobility protocol on top of access authentication. Drawbacks of this approach have been described, e.g. in [13]. One solution is to integrate access network access control with the mobility protocol. The secure proxy mobility protocol ProMPt [14] which will be described in the next section follows this approach.

3 THE PROXY MOBILITY PROTOCOL

In this section the proxy mobility protocol (ProMPt) is explained briefly together with its security functionality.

3.1 Scenario

The scenario as shown in Figure 1 assumes IP communication between a mobile node (MN) and a corresponding node (CN). The mobile node is assumed to move within one mobility domain which is separate from the home domain in which home agent (HA), authentication, authorization and accounting server (AAA) and the home support services (HSS) reside. The mobile node's link layer terminates at an access router (AR). Within the mobility domain there is one mobility anchor point (MAP), which serves as a router for all communication from and to the mobile node. The MAP keeps state of which access router the mobile node is currently attached to. Packets addressed to the mobile node are tunnelled to the appropriate access router and delivered to the MN. While moving within one mobility domain, the mobile node keeps the same IP address.

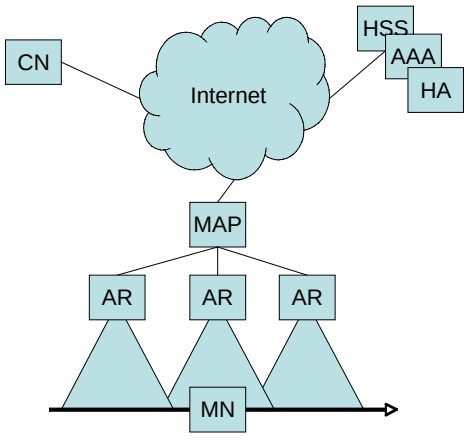

Figure 1: Usage scenario for ProMPt. A mobile node moves within one mobility anchor point's domain covered by several access routers.

3.2 Protocol Operation

3.2.1 Mobility

The AR maintains a table mapping the IP address to the link layer address for each of the MNs it currently serves. The AR is responsible for updating the MAP with information which MNs it serves. For the link the AR serves, it also acts as proxy for all off-link mobile nodes, i.e. mobile nodes registered with the MAP but not on the same link. This in effect turns the whole mobility domain into one virtual link layer domain.

The MAP maintains a route to the AR for all MNs it currently serves. Packets between the MAP and AR are tunnelled using existing tunnelling mechanisms. All communication of a MN with a correspondent node in the Internet goes through the MAP.

3.2.2 Authentication

Authentication in ProMPt is based on the Authentication and Key Agreement protocol AKA which is also used in 3G networks. It is therefore possible to reuse the same infrastructure, thus fulfilling one of the main design goals stated in the Introduction. While AKA runs directly in 3G networks, in WLANs using IEEE 802.1X it is encapsulated in EAP as Extensible Authentication Protocol-Authentication and Key Agreement. AKA is based on symmetric cryptography. This has the disadvantage of requiring a shared secret, but the advantage of not being very demanding on processing power. To counter the disadvantage 3G makes use of tamper resistance hardware in the form of SIM where the shared secret is stored.

3.3 Message Sequence

3.3.1 Initial Attachment

The initial attachment makes use of a modified EAP-AKA based mutual authentication. The radio access network (RAN) is selected by the MN on the start-up.

The MN finds and connects to a RAN based on RAN specific technology. Authentication is performed using EAP. The network access identifier of choice is the temporary mobile identity TMSI, in cases when it is yet unknown, the permanent IMSI is used. As in normal EAP-AKA, the authenticator, i.e. the access point if the RAN technology is wireless LAN, relays the EAP message to the AAA server that checks the availability of Authentication Vectors (AVs) which the Home Environment (HE; this includes the home subscriber subsystem etc.) can provide if necessary. AVs contain all information necessary for an authenticator to successfully perform mutual authentication with MN. Once the AR knows the AV, AKA based mutual authentication takes place. After successful authentication further AVs are sent to the MAP and cached there. On every authentication/re-authentication the MAP checks the number of cached AVs and requests more if the number falls below a given threshold.

If the MN is attached to a 3G network, key establishment is performed as normal. In case of IEEE 802.11, IEEE 802.11i key generation is used. After successful completion of EAP-AKA, the AR assigns an IP address to the MN. This IP address is reported with the corresponding TMSI to the MAP where it is stored. This concludes the initial step of ProMPt.

3.3.2 Handover

There are two types of handover, scheduled and unscheduled. In scheduled handover the MAP takes the decision to hand over to a different access network based on periodic measurement results reported by the MN and AR. The algorithm to select the target AR can be arbitrary and take into account parameters like signal strength, AR load distribution, handover history, etc. In unscheduled handover the MN takes the decision to hand over to a different RAN based on sudden changes in connectivity.

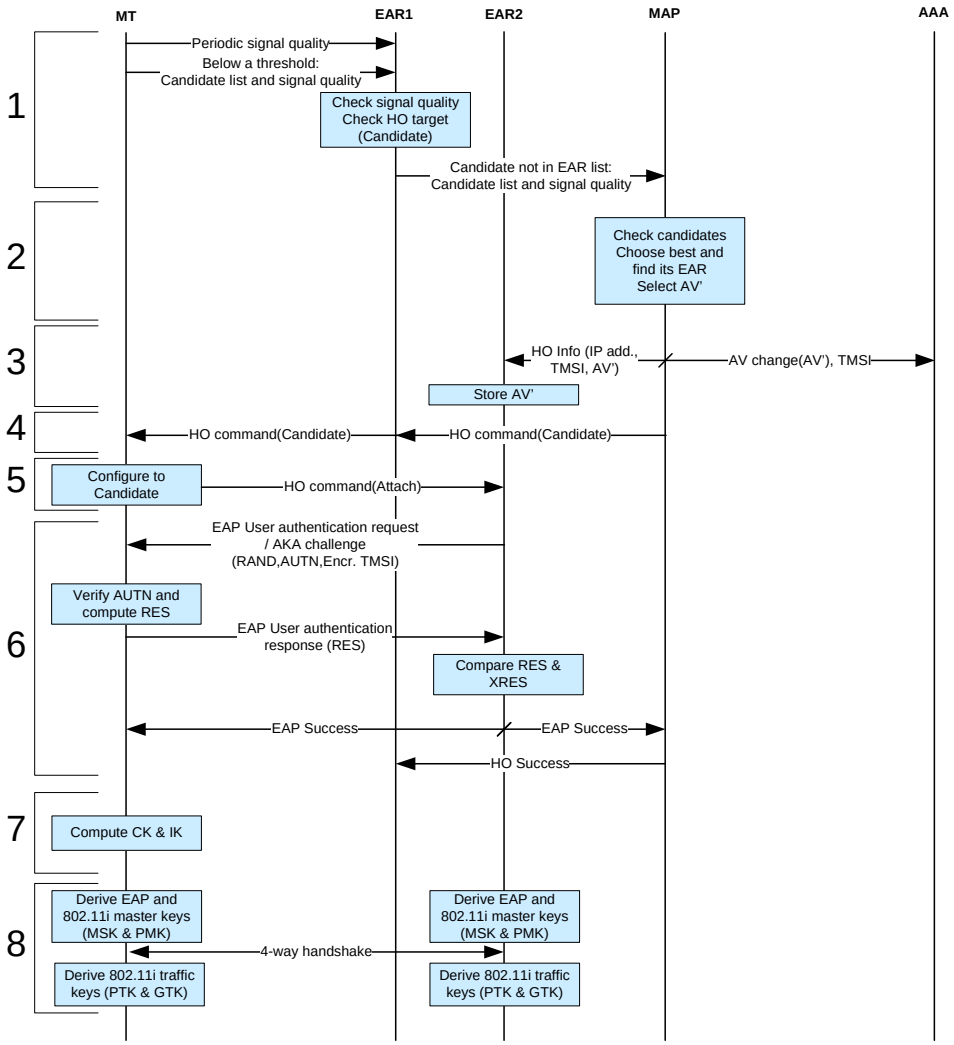

Figure 2: Message sequence for scheduled handover

For scheduled handover (see Figure 2), after the MAP decides to execute a handover, it informs the target AR, including an AV in this message. The MAP then sends a handover command to the MN, which contains all required information. Based on this the MN contacts the new AR. Mutual authentication takes place between the AR and MN without requiring the AR to retrieve AVs during the exchange. Key establishment is done as in the initial attachment process. After successful authentication, the previous AR and the MAP are informed, the MAP and previous AR update their databases.

After the handover decision is made, the MAP informs the target AR of the MN together with new AV and the MN IP address. The MN is sent a handover command from the MAP together with any required information based on which the MN contacts the new RAN. Then mutual authentication takes place as in AKA but without the necessity of the target AR retrieving AVs. Key establishment is done as in initial attachment. The current AR sends a HO success message to the MAP and the previous AR. This notification at MAP triggers the ProMPt mechanism, i.e., the MAP registers the new location of the MN and the old AR removes the MN records from its database.

In unscheduled handover (see Figure 3) the MN sends the initial handover command. The procedure is similar to the procedure for scheduled handover. The difference is that the new AR now indicates to the MAP the fact that it received a handover command. The MAP then provides the AV and handover continues as described for the scheduled case.

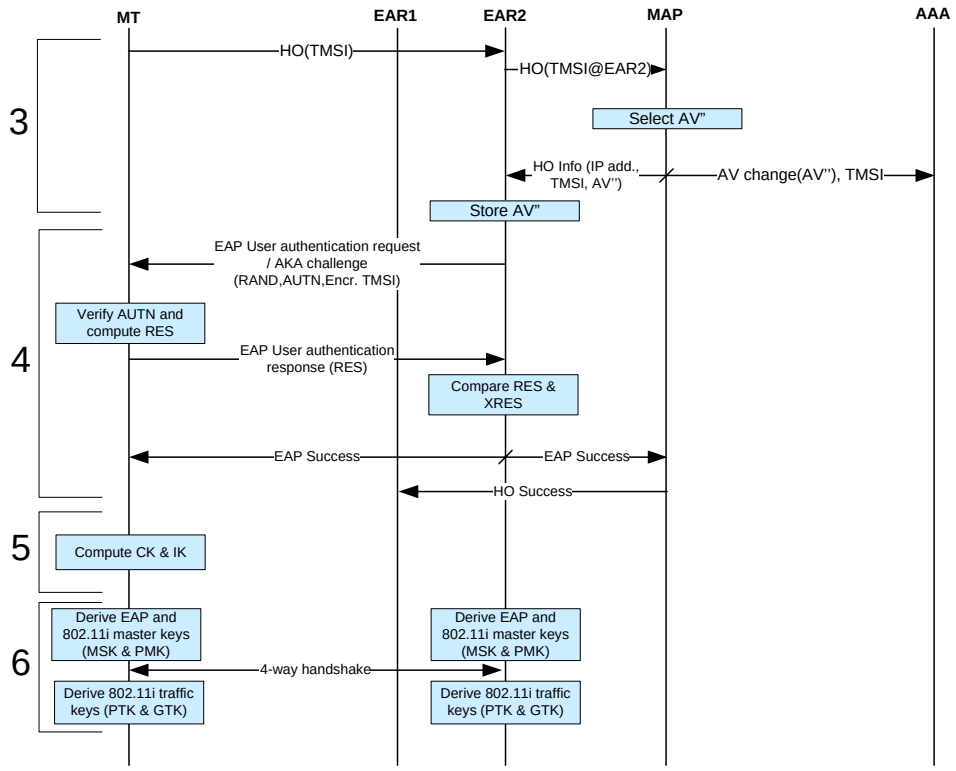

Figure 3: Message sequence for unscheduled handover

3.4 Security Observations

In this place we only provide some observations on the security of ProMPt. A thorough analysis is given elsewhere [14].

ProMPt relies heavily on security domains. AVs are passed around relatively freely in the access network. The access network and all its entities must be secured against attacks, otherwise these AVs could be misused for man in the middle attacks. The MAP stores a large number of AVs and therefore would make a prime target for an attack. Invalidation of AVs stored in the MAP has not been addressed, yet. The current assumption is that these AVs have a certain lifetime after which they expire. The lifetime of the AVs distributed to the AR can be even shorter, as they are distributed only on demand. Operational security of access routers needs to be ensured. A subverted AR could be used to extract AVs from the MAP.

4 SIMULATION TESTBED

The purpose of the simulation test bed is to determine the performance of the proposed solution. The setup consists of 6 laptops (IBM Thinkpad X41) running FreeBSD6.0. One laptop simulates the mobile node (MN), two laptop represent access routers (AR), one performs the functions of the mobility anchor point (MAP), one is the correspondent node (CN), and one computer represents home agent (HA), authentication server (AAA), and home subscriber server (HSS).

Each one of these machines run a python script that runs the protocols involved. At the moment the simulator runs the message sequence, with detection for message mismatches due to message loss or programming errors. Parameterized sleep periods simulate the actual processing. This setup allows rapid changes in the protocol design. See Table 1 for command in a control block of a message exchange in a protocol definition.

Table 1: Statements in simulator control block

name1 name2	Message sender and receiver
message *messagetext*	Text to be sent
layer *#n*	Layer on which message is sent (important because of different routing behaviour)
delay *#n*	Sleep for n microseconds after reception of message (to simulate message processing)
timeout *#n*	Timeout on receiving side after *n* seconds
execute *command*	Execute operating system command *command*. Used for setting routes.

Connectivity between the computers is via a 100Mbit/s Ethernet switch. The characteristics of the connections between the computers are adjusted to emulate real behaviour using *dummynet*[15]. *Dummynet* extends the *ipfw* IP firewall packet filter. Packets processed by *dummynet* can be delayed by a specified time. Bandwidth of links can be limited. These features are used to get realistic and reproducible system behaviour. The delays set are 100ms for $\tau_{Internet}$, 10ms for τ_{Domain}, and 0.1ms for τ_{Access}, representing the delays between hosts in the Internet, access routers and the MAP, and the mobile node and access routers respectively. Bandwidth limitation is not used.

Changing the routing tables in the MAP, AR1, AR2 and the MN simulates mobility. Schematically, this is represented as switches in Figure 4. Routing entries in AR1 and AR2 can be switched to “off” and “through”, while routes at the MAP and MN can be “off” or go either via AR1 or AR2.

Performance measurements are done using iperf between MN as client and CN as server. For TCP throughput measurements, window size is left at the default value, result binning is at 0.5s intervals. For UDP throughput measurements the sending throughput is set to 5Mbit/s, A small python script measures UDP packet loss for voice over IP like traffic (160byte packets every 20ms). In addition, the simulator measures the time to complete the protocol.

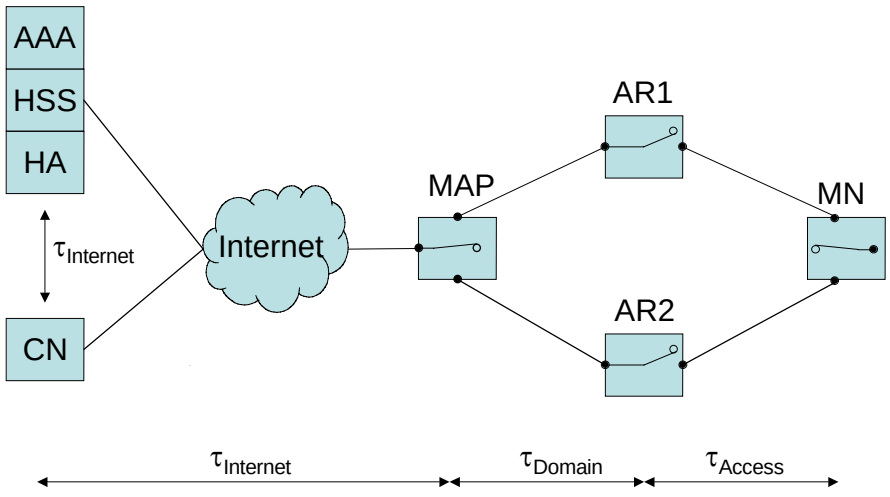

Figure 4: Schematic view of simulator

Measurement runs show 8 handovers forward and backward between AR1 and AR2. For TCP measurements the handovers occur approximately every 10s to give the flow control the possibility to stabilize again. UDP does not have flow control, therefore this interval could be set to 5s for the UDP tests.

To be able to gauge the quality of improvement of ProMPt, a simulation of an authentication with EAP-AKA followed by handoff using mobile IPv6 was run as reference.

5 SIMULATION RESULTS AND DISCUSSION

Table 2 shows aggregated results from the simulation runs. It can be seen that, as expected, ProMPt scheduled handoff performs better than ProMPt unscheduled handover, which is more than ten times faster than the reference mobile IPv6 with EAP-AKA. The difference between scheduled and unscheduled handover is almost exactly one round trip time between AR and MAP, which is the time the target AR takes to fetch the AV.

Packet loss rates for the reference show one speciality: uplink and downlink are different. This is due to the fact that after completion of EAP-AKA the client can send to the server, while the downlink needs to wait for reception of the binding update message of the mobile IP protocol to be able to start sending.

The packet loss rates are not quite as low as one would have expected from the protocol completion times. This is due to the fact that the simulator scripts call the system command “route” to edit the routing tables. Linear regression of the results shows that approx. 5 packets get lost during the route switching process. This leads to the conclusion that the simulator should be updated to interface directly with the routing tables of the OS.

Therefore, the throughput measurements can only be interpreted with caution. Typical results of a test run are shown in Figure 6 for scheduled handoff, Figure 7 for unscheduled handoff and Figure 8 for the reference run of EAP-AKA with mobile IPv6.

It can be seen that TCP performance reaches a maximum throughput of approximately 1Mbit/s. UDP throughput, however, easily reaches 5Mbit/s. This is an indication that the default maximum TCP window size is set too small for high latency links.

The saw tooth shape of the throughput curves originate in TCP’s slow start mechanism. As expected from the discussion about the packet loss rates, differences between scheduled and unscheduled handoff are almost invisible. The big difference that is visible between these two and the TCP throughput rate with the reference handover most likely stems from the fact that the long delay until connectivity is restored triggers TCP’s retransmission timer RTT.

As expected, The UDP throughput measurements show no noticeable difference between scheduled and unscheduled handover. Some differences are visible with regard to the reference handover.

Table 2: simulation results

	Time for protocol completion	Packet loss
ProMPt scheduled handoff	0.048s ± 0.001s	8±1
ProMPt unscheduled handoff	0.071s ± 0.002s	10±2
Mobile IPv6 with EAP-AKA	0.97s ± 0.01s	23±1 uplink 59±2 downlink

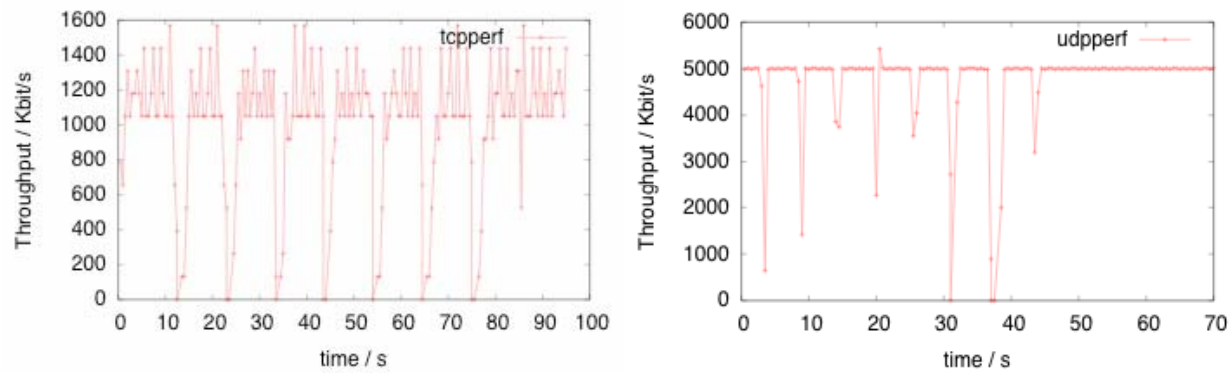

Figure 5: Throughput with ProMPt scheduled handover

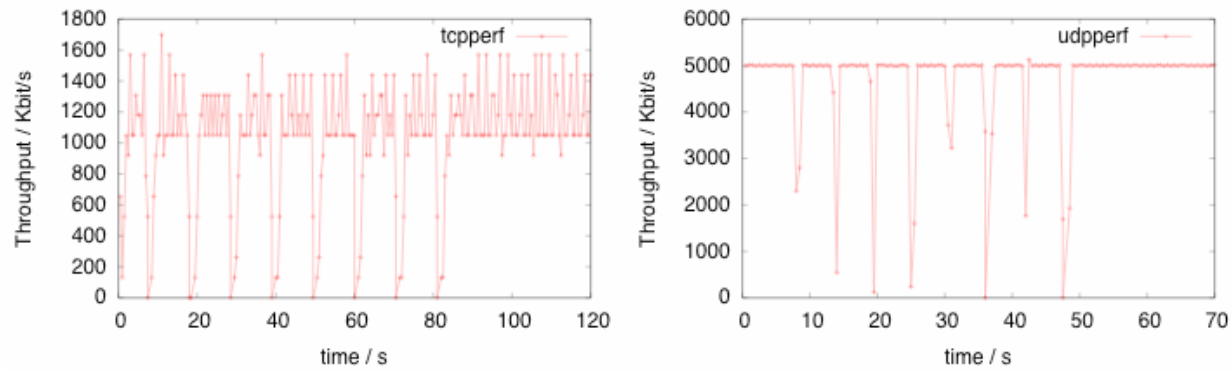

Figure 6: Throughput with ProMPt unscheduled handover

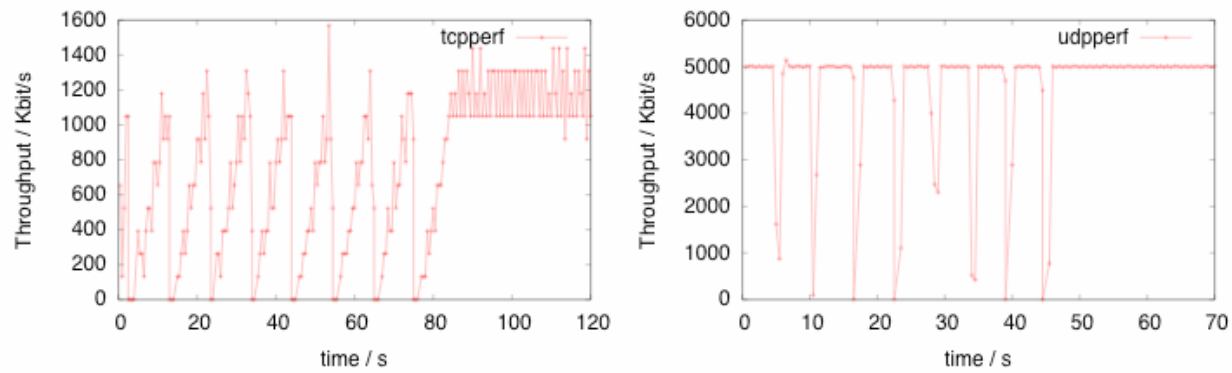

Figure 7: Throughput with EAP-AKA and mobile IPv6

6 CONCLUSIONS AND OUTLOOK

This paper compares performance of two handover mechanisms (ProMPt and Mobile IPv6) as measured in our simulation testbed. The benefits of ProMPt are clearly visible. Handover times for scheduled ProMPt are 50ms for scheduled handover and 70ms for unscheduled handover while Mobile IPv6 takes almost 1s for handover with route optimization when the home agent is far away. Despite the fact that the simulator's route switching speed dominates handover times for ProMPt, we still obtain good performance.

Therefore, it is probably the case that a real PromMPt deployment would achieve better performance. In addition, the ProMPt solution would certainly benefit from buffering of packets sent to the MN. This would reduce the packet loss to which upper layer protocols (e.g. TCP or real time applications) are especially sensitive. Such buffering would ideally take place at the MAP because it is a fixed point on the path followed by packets. One can continuously buffer packets

using a sliding window long enough to store all packets received during handover. This would improve performance for both scheduled and unscheduled handovers.

The simulator has proven a useful tool for the quick evaluation of new handover mechanisms. The obvious next step is to improve the interface of our simulator with the routing tables in the underlying operating system.

7 REFERENCES

[1] C. Perkins, Ed. IP Mobility Support for IPv4, Internet Engineering Task Force Request for Comments RFC 3344. Available at http://www.ietf.org/rfc/rfc3344.txt

[2] C. Perkins, D. Johnson, and J. Arkko. IP Mobility Support in IPv6, Internet Engineering Task Force Request for Comments RFC 3775. Available at http://www.ietf.org/rfc/rfc3775.txt

[3] R. Koodli, Ed. Fast Handovers for Mobile IPv6, Internet Engineering Task Force Request for Comments RFC 4068. Available at http://www.ietf.org/rfc/rfc4068.txt

[4] H. Soliman, C. Castellucia, K. El Malki, and L. Bellier. Hierarchical Mobile IPv6 Mobility Management (HMIPv6). Internet Engineering Task Force Request for Comments RFC 4140. Available at http://www.ietf.org/rfc/rfc4140.txt

[5] A. G. Valko. Cellular IP: A New Approach to Internet Host Mobility. *ACM Comp. Commun. Rev.*, Jan. 1999.

[6] R. Ramjee *et al.* HAWAII: A Domain-based Approach for Supporting Mobility in Wide-area Wireless Networks. *Proc. IEEE Int'l. Conf. Network Protocols*. 1999.

[7] C. Keszei, N. Georganopoulos, Z. Turanyi, A. G. Valko. Evaluation of the BRAIN Candidate Mobility Management Protocol. IST Mobile Communication Summit, September 2001.

[8] K. Boman, G. Horn, P. Howard, and V. Niemi. UMTS Security. *IEE Electronics & Communication Engineering Journal*, Oct. 2002.

[9] B. Aboba, *et al*. Extensible Authentication Protocol (EAP). Internet Engineering Task Force Request for Comments RFC 3748. Available at http://www.ietf.org/rfc/rfc3748.txt

[10] B. Aboba and P. Calhoun. RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP). Internet Engineering Task Force Request for Comments RFC 3579. Available at http://www.ietf.org/rfc/rfc3579.txt

[11] B. Aboba and D. Simon. PPP EAP TLS Authentication Protocol . Internet Engineering Task Force Request for Comments RFC 2716. Available at http://www.ietf.org/rfc/rfc2716.txt

[12] J. Arkko and H. Haverinen. Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA). Internet Engineering Task Force Request for Comments RFC 4140. Available at http://www.ietf.org/rfc/rfc4140.txt

[13] Anand R. Prasad, Alf Zugenmaier, and Peter Schoo. Next Generation Communications and Secure Seamless Handover. *Proc. SecQoS Workshop at IEEE SecureComm*, 2006.

[14] J. Laganier, *et al.* Secure ProMPt: Secure Seamless Mobility and Handover in B3G All-IP Networks. Under submission.

[15] L. Rizzo. Dummynet: a simple approach to the evaluation of network protocols. *ACM Computer Communication Review* 27, Jan. 1997.