Challenges for Handovers in Hybrid Networks

Kira Alexandra Kastell

Abstract—**Hybrid networks are built from different loosely coupled access networks. In contrast to heterogeneous networks there is no additional interworking entity. In hybrid networks not only the handover protocols and air interfaces differ but also the authentication and credentials. We propose a hybrid handover protocol that, without the need of major changes of existing standards, copes with the different protocols and includes mandatory authentication. This is a prerequisite for hybrid handovers especially if more than one provider is involved. The protocol has been evaluated by simulations implementing GSM, UMTS, and Wi-Fi. Results show a handover success rate of more than 90% in GSM and UMTS and up to 85% in Wi-Fi. The success rate only decreased slightly compared to conventional handover without authentication. If authentication is included in conventional GSM or UMTS handovers their success rate is only about one third of the one for the hybrid handovers presented here.**

***Index Terms*—Authentication, handover, hybrid networks.**

I. Introduction

Mobile communication networks and systems are the most popular means for telecommunication as they are comparatively easy to install. With an increasing number of mobile networks - everyone with a higher data rate as the ones before - users get accustomed to the ever increasing availability and quality of mobile connections. Ongoing research aims to provide better and better communication experience for the user and to fulfill his needs for ubiquitous availability and reliability with growing data rates.

Nowadays we have a broad variety of already existing networks, among them popular systems such as GSM, UMTS, and Wi-Fi (IEEE 802.11b) as well as emerging ones as WiMAX. These networks differ in many ways: frequency bands, bandwidth, modulation scheme, range of a single transmitter, type of coverage (island or nationwide), subscription mode, protocols, security features and keys, and many more. Most of these networks have been designed independently from each other.

The short-term way to provide the user with the experience desired is to enable the different existing systems to interoperate in a way that the user can start a communication in either network and will be seamlessly transferred to a better fitted network if this becomes available without noticing the change of the underlying communication system. This is a big challenge as the protocols and interfaces of the different systems are not designed for interoperation.

Especially for well established communication systems with a large subscriber base and thousands of network access points (NAP) a change of the interfaces would be too expensive. The immense costs also prohibit the deployment of one new communication system substituting all existing networks. This is the reason why research focuses on new inter-working modules for existing systems. In different approaches the inter-working takes place at different levels. There is no single best solution as the trade-off between the complexity of the inter-working protocol and necessary changes in the network entities and protocols have to be dealt with. Considering the aspect that the inter-working at best should cover all existing and future networks these solutions are preferable that do not rely on (major) changes in the standardization. This means that no direct inter-working - with an additional entity - can be established. That will probably lead to more complex inter-working protocols but prevent the systems from hardware changes. Software changes can be kept to a minimum if the inter-working protocol takes advantage of tunneling mechanisms for parallel control communication with different air interfaces and protocol systems. The result is a so-called hybrid network discussed in this paper.

The critical path for mobile network interoperability is the handover. It needs to be executed fast and unnoticeable for the user. Hybrid handovers aim for inter-working of completely different networks and therefore face at least the following challenges: duration of the handover and its execution, transfer of credentials while maintaining the expected level of network and data security and of course choice of the best suited network to handover to.

The remainder of the paper is organized as follows: In section II existing handover procedures are analyzed to identify the most critical steps. In section III the special challenges for hybrid handovers and a concept to handle these are introduced. Simulation details for the concept evaluation are given in section IV. In section V the simulation results are presented before section VI concludes the paper.

II. Existing Handover Procedures

The term handover in the narrower sense only refers to circuit switched networks. In this paper for better legibility handover shall also cover the relocation procedure in packet switched networks. Handover procedures here are defined as procedures that allow a user to seamlessly use services while changing from one network access point (NAP) to another. For it no user interaction is required, the rerouted connection is neither lost nor interrupted and in the ideal case the user does not even perceive the change of network access. Therefore

Manuscrito recebido em 15 de julio de 2011; revisado em 18 de novembro de 2011.

K. A. Kastell (kastell@fb2.fh-frankfurt.de) works with Fachhochschule Frankfurt am Main – University of Applied Sciences. Nibelungenplatz 1, 60318 Frankfurt am Main, Germany.

handover latency is a critical issue even in intra network scenarios.

Mobile networks can be grouped into two categories: On the one hand area-wide networks with a built-in handover procedure, e.g. GSM, UMTS; on the other hand wireless networks primarily aiming for short-range communication in a well defined and mostly small area with only one NAP or few NAPs strongly interconnected with each other, e.g. Wi-Fi, WiMAX. These systems have been further developed and now enable handovers between their NAPs. But the way the handover is executed and the security mechanisms differ widely from the systems inherently designed for handover making it more difficult to design a hybrid handover especially when security plays a role. Moreover there is no change foreseen in the wireless interface during the handover - except where one communication system is the designated successor of another.

A. *Mobile networks with built-in handover*

Figure 1 depicts the Inter-MSC handover in GSM [1]. This handover serves as a basis for the hybrid handover. It is a so-called mobile assisted handover as the handover decision itself is taken by the fixed network components but relies on measurement data provided by the mobile station (MS). Despite slightly different names for the commands the UMTS [2] and cdma2000 [3] handovers look alike. Thus, our results generalize to these cases.

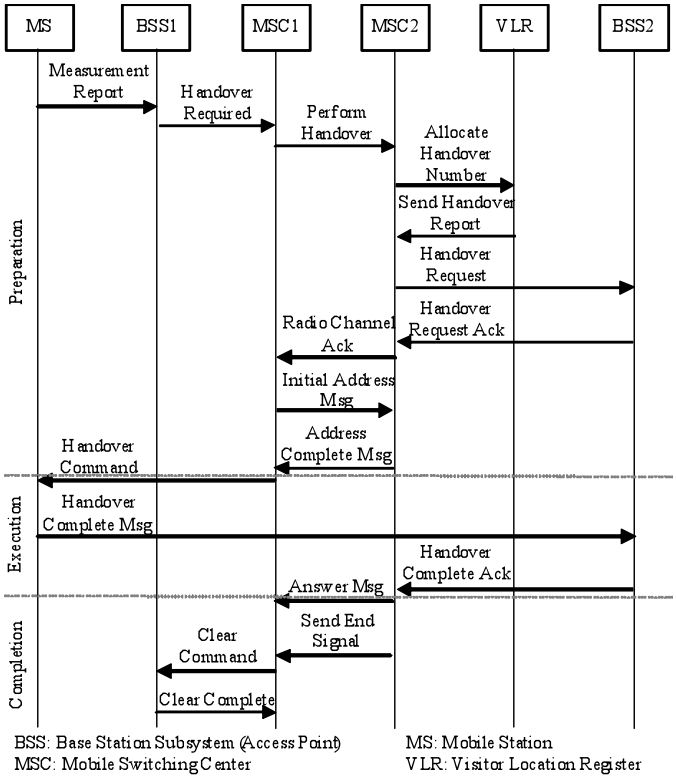

Fig. 1. Inter-MSC handover. [cf. 1]

The handover can be divided into three phases. The first and most time consuming phase is the handover preparation (which ends with the address complete message). The subsequent handover execution starts with handover command and stops with handover complete message. Between these two messages the MS has not established any connection to any NAP. All messages after the handover execution belong to the handover completion phase. They have to be performed to release resources but do not contribute to the handover latency.

All messages up to and including handover command need to be executed while the MS moves inside the overlapping coverage area of the two NAPs involved. The size of the overlapping area depends on the network planning and the placement of the NAPs. The duration of stay then also depends on the speed of the MS and how it crosses the cell border (perpendicular or along the border line).

The single message measurement report in figure 1 refers to periodically transmitted information gathered by the MS about the field strength of (up to seven) neighboring NAPs. To be able to detect these NAPs the MS needs to be close enough to them, e.g. close to the border of its serving cell. Handover required indicates that the serving NAP provides a weaker field strength level to the MS than the target NAP. This means that it already has been identified that there is a risk of losing the ongoing connection. Handover becomes even more urgent as networks typically take into account a certain margin up to which the serving NAP may be weaker than its neighbor to prevent frequent (ping-pong) handovers at the borders between two cells. As the measurement reports are sent in periods of at least 480 ms [5] and the handover decision is taken based on several consecutive reports it is obvious that handover preparation often is more time-critical than the handover execution. As the available amount of time strongly depends on the coverage and overlap areas, network planning will play an increasingly important role for the integration of hybrid systems.

B. *Mobile networks with later added handover*

Later added handovers often look like a workaround solution. In Wi-Fi (IEEE 802.11b) the MS scans, either actively or passively, for available NAPs (cf. fig. 2a) in the handover preparation phase. The handover execution phase consists of a procedure similar to an initial association with any NAP. There is the opportunity to exchange credentials between the NAPs involved in the handover, but the release of resources is not specified.

In WiMAX the handover procedure looks even more complicated as the exchange of credentials and other information only is started after the necessity of a handover has been indicated. Therefore the procedure has a higher overall latency. The handover preparation has fewer messages than in GSM. However, the handover execution is a bit longer. The authentication is mandatorily included in the handover completion phase. This makes the WiMAX handover safer than the one in GSM but weaker than the one in Wi-Fi where the authentication with the new NAP has to take place before the handover execution.

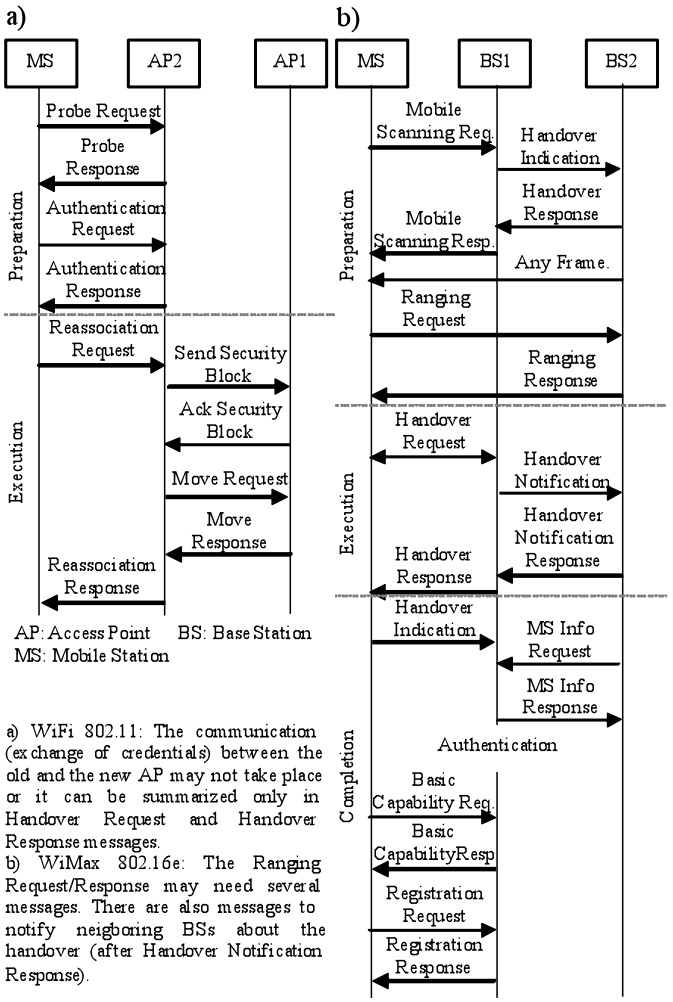

Fig. 2. a) Extended 802.11 handover [6-8], b) 802.16e handover [9-10].

III. CONCEPT FOR HYBRID HANDOVERS

A. Challenges for handovers

A closer look at the overall handover process is needed. The real execution phase from handover command to handover complete is pretty fast and nothing can be added in between without the user noticing it. So the additional tasks have to be fulfilled before the handover execution phase starts or immediately afterwards. But authentication with the new system before the user enters it would provide the strongest security, although authentication today of course is also performed after entering the system, e.g. if a user powers up his mobile. Then an unsecure connection is established first, immediately followed by authentication at least of the user (e.g. GSM), preferably mutual (e.g. UMTS). Therefore we focus on the handover preparation phase not only because this is where mandatory authentication with the new NAP has to be integrated if the security level of each system shall remain the same as in the single network case but also because it is the most time consuming handover phase. If the authentication takes place after the handover the credentials first have to be converted and give to the new network before this network can use its own credentials. This at least weakens the portion of communication processed between handover and new authentication.

The built-in handover has latency low enough to cope with the requirements for mostly unnoticeable handovers. This is bought dearly as the low latency only can be achieved because there is no authentication between new NAP and MS included in the handover procedure. This at least weakens the security of the new connection but might also weaken the security of the former connection by reverse engineering the keys used. Then recorded traffic can be deciphered.

During a handover in a single network it might be assumed safe to trust in the previous authentication as all components belong to the same network and share the same credentials. But the missing authentication weakens the security level if different networks (with different security features) are incorporated. Even performing a handover between GSM and UMTS weakens the enhanced security mechanism of UMTS. GSM only uses one 64 bit key K_c for authentication of the mobile to the network, while UMTS uses two keys for ciphering (CK) and integrity (IK) and mutual authentication, each consisting of 128 bits. They different keys used for GSM are simply converted into UMTS keys and vice versa by public formulas:

$$K_c = c_3((CK, IK) = CK_1 \oplus CK_2 \oplus IK_1 \oplus IK_2 \quad (1)$$

$$CK = c_4((K_c) = K_c \,||\, K_c \quad (2)$$

$$IK = c_5(((K_c) = K_{c1} \oplus K_{c2} \,||\, K_c \,||\, K_{c1} \oplus K_{c2} \quad (3)$$

With $K_c = K_{c1} \,||\, K_{c2}$ and K_{c1} and K_{c2} each consist of 32 bit. CK and IK are split into CK_1 and CK_2 and IK_1 and IK_2 respectively, each consisting of 64 bit, so that $CK = CK_1 \,||\, CK_2$ and $IK = IK_1 \,||\, IK_2$.

This weakens UMTS security as the security algorithms of GSM are broken and the key K_c can easily be derived from a few milliseconds of encrypted traffic [11]. If this weakness occurs in systems designed to work together, missing authentication in hybrid networks will have more severe consequences. Thus, for real hybrid scenarios consisting of networks that have not even been designed for inter-working, missing authentication will prevent providers from implementing inter network handovers.

The later added handovers perform the setup of a new connection and therefore include complete authentication. But this slows them down. In addition as no regular measurement period of surrounding NAPs is included the scanning of the environment also contributes to a very high latency.

If the handover latency itself in every contributing network will be kept below the recommended 50 ms [12] or just below 200 ms [4] for unnoticeable interruption from which we are still far-off according to table I this will still not necessarily lead to affordable durations of hybrid handovers. But the preparation has to be performed faster than before, especially if the cells get smaller and the available time for preparation therefore is very short.

TABLE I
LATENCIES IN HANDOVERS OF DIFFERENT NETWORKS [5, 7, 9, 13].

NETWORK	HANDOVER EXECUTION	MINIMUM LATENCY	MAXIMUM LATENCY
With preliminary measurements, theoretical values from standardization			
GSM	460 ms	1920 ms	2500 ms
UMTS TDD-TDD	464.9 ms	944.9 ms	944.9 ms
UMTS TDD-FDD	434.95 ms	2615.95 ms	6977.95 ms
UMTS FDD-TDD	734.95 ms	1934.95 ms	7934.95 ms
UMTS FDD-FDD	734.95 ms	1214.95 ms	6734.95 ms
Without handover preparation and authentication (measured)			
WLAN 802.11		35 ms	430 ms
WiMAX 802.16e		100 ms	750 ms

The most critical phase in terms of time consumption is the handover preparation, e.g., the detection that a handover is necessary and the derivation of the target cell. Table I shows that the time for measurements depends on the network topology and the transmission mode. For measurement purposes the MS needs an unoccupied air interface. Therefore TDMA (time division multiple access) scenarios are better suited as there are always free timeslots in which the MS is not allowed to transmit and does not need to receive so it can perform measurements even if switching to another air interface is necessary. CDMA (code division multiple access) scenarios with FDD (frequency division duplex) - which are preferable in terms of spectral efficiency - need to add a special measurement mode. In UMTS this so-called compressed mode creates free timeslots by compressing transmission data and taking advantage of the time gained by compression to change the air interface. As compression in a well-designed network will not be able to save a lot of time, compared to TDMA systems the measurement period needs to be expanded even if only one network is involved.

Measurement problems will arise in hybrid networks as the very nature of them is the difference in air interfaces. Thus, for every measurement the air interface has to be switched making measurements more complicated and time consuming. Furthermore, there are more cells to be measured as there are more networks involved. The number of neighboring cells increases as the different networks overlap. The MS should at least measure the (seven) best serving NAPs in its own network plus all NAPs of other networks having higher field strength than the weakest measured NAP of the own network. A problem is that the MS initially does not know which other networks might be available. Here some broadcast information based on measurements of other MSs or the NAPs themselves could shorten the process. If available network types are going to be broadcasted it will prevent the MS from powering up and measuring air interfaces for which no NAPs are available at the present location. But in general hybrid handovers still are more time consuming as they do not only incorporate a change of frequency and/or coding but also a change of the air interface. This mostly means powering down one and powering up the other air interface as simultaneous use consumes too much power (and needs hardware with more than one receive/transmit path). Therefore a new concept for the derivation of the target cell is needed. This should be based on less or faster measurements to gain additional time for authentication.

To guarantee the same security level as before authentication must be added before the handover execution is completed. If the authentication request is not sent before the handover complete message one or two messages exhibit weaker security. In this case the overall handover latency is extended but the connection will not be lost as the authentication adds the delay after handover execution. But the new network needs a buffer to store incoming data during the authentication procedure. This is why authentication should take place before the handover execution.

Another challenge is the protocol itself. If the changes in standardization should be kept to a minimum tunneling and transport of messages through the backbone network instead of over the air interface is preferable.

B. Proposed solution for location-based hybrid handovers

The proposed protocol includes mandatory authentication with the new NAP. The messages between MS and new NAP are tunneled via the serving NAP. The serving NAP just forwards the messages and does not need to be able to understand the content of the message. So, credentials of any standard can be contracted by MS and new NAP using the algorithms of the network to which the handover shall be performed.

The latest moment for really secure authentication is between handover command and handover complete. But as authentication takes in between 500 ms and approximately 2 s handovers will fail if the authentication is initiated that late. On the other side authentication can only start after the target network or target NAP is known as otherwise authentication to all neighboring networks would be necessary. This will produce an overhead that is far too high. Therefore we need information about the target cell to perform a proactive authentication. If the target cell is known (well) before the handover becomes necessary, target-oriented authentication could be initiated using the tunnel via the serving NAP.

To determine the target cell or network in advance the measurements for handover preparation need to be revised. The measurements or scanning processes in state-of-the-art handovers are very time consuming. Additional measurements as stated above will lead to even longer handover preparation. This will result in handover failure as the overlapping areas between adjacent cells will not grow wider rather they will shrink. Thus, the amount of measurements can not be increased but the existing measurements have to be used to calculate the information needed.

The network and its NAPs could be provided with information about neighboring networks to support the MS with a list of networks to measure. On the other hand the measurements inside one network can most often provide enough information to calculate the position of the MS relative to the serving NAP and the neighboring NAPs. In nearly every network the MS measures received field strength values from surrounding NAPs. Measurements from a single network can be used to calculate the position of the MS. So the measurements in hybrid systems will be sped up because only on air interface will be involved. From consecutive

measurements and the corresponding consecutive positions the target cell may be derived. The choice of the target cell can be enhanced if the topology of all networks constituting the hybrid network is known and available to all sub-networks. This knowledge can be used by the serving network to choose a target cell based on the position of the MS. We could show that not even the absolute position but only the position relative to the neighboring cells has to be known [14]. This can easily be extracted even from a subset of field strength measurements. With additional information about the topology of all available networks the amount of measurements may also be further reduced in the future.

Depending on the velocity and mobility scheme of the MS the position can be calculated well in advance of the handover. Then proactive authentication with the target cell can take place and also handover preparation and reservation of resources can be initiated. In a second step the knowledge of the location may even help to prevent the MS from some measurements as the location may indicate the best target network and NAP. Then the MS only needs to confirm that with one single measurement instead of measuring all surrounding NAPs.

C. *Protocol*

The proposed procedure for hybrid handovers employs the existing handover protocols. There are no changes in the protocols themselves but whenever the handover preparation requires contact to the target network the messages are tunneled by the serving NAP and transferred to the target NAP. This only adds a small latency as there are no new messages but only new addresses in the header, but it depends on the routing in the backbone network. The hybrid protocol follows the protocol of the serving network up to and including the message handover command, reassociation request or handover indication. After the handover execution the protocol follows the procedure of the target network. The new NAP informs the former NAP about the successful handover. Then the old NAP releases its resources. The serving NAP takes the roll of a switching point between MS and target NAP. Higher overall latency may result if the route through the backbone networks is considerably longer than the one between the NAPs of one single network.

The hybrid handover protocol for two GSM networks is shown in figure 3. The measurement reports for handover preparation can be reduced by using location-based cell prediction. This location-based cell prediction based on measurements in one single network can save at least 480 ms, most of the time it saves more than 1 s [14]. In most of the cases, this gives time to include and complete mandatory authentication before the handover execution. If only 480 ms can be saved, some problems may occur, because authentication takes about 500 ms to 2 s, depending on the target network. GSM is the fastest; IEEE 802.11 and WiMAX are the slowest ones. But this problem also can be dealt with without major changes in the protocol (see below).

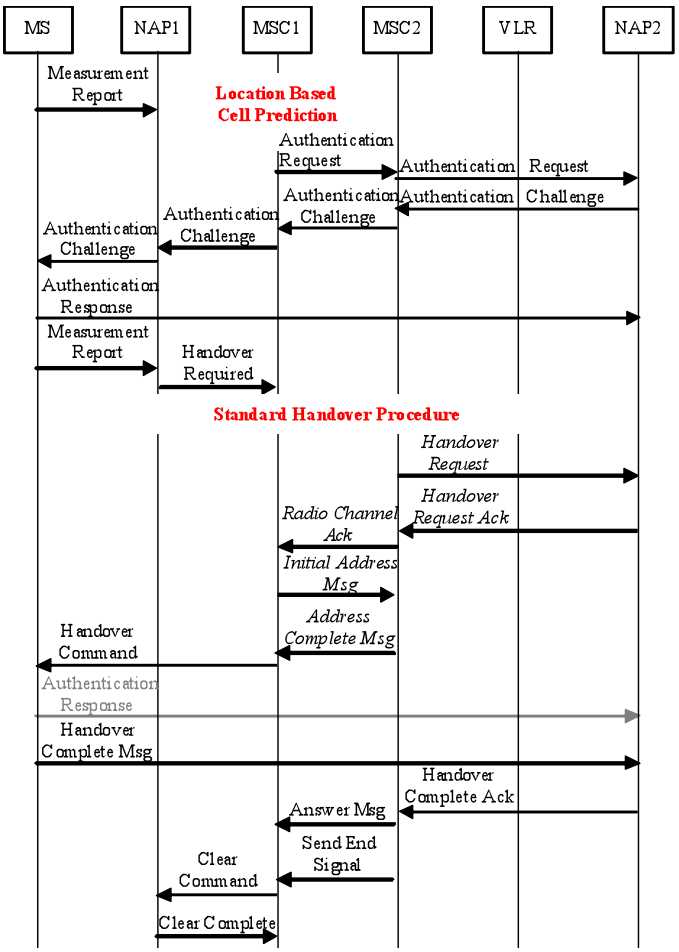

Fig. 3: Handover with pre-authentication. The commands in italics can also be performed in advance, but they then may occupy additional resources.

The included authentication guarantees that the security of each contributing network is not affected. Thus, each single network always has its built-in security and is never weakened. But the overall security of the hybrid network still depends on the contributing networks. The proposed handover protocol does not establish one single overall security level. It only prevents lack of security in the single networks. The authentication is performed using the protocol of the target network. Therefore the security level of the target network is guaranteed after the handover. The messages are tunneled by the serving NAP.

It can be noticed that the authentication response should be sent before the handover command. However if the remaining time is too short, the authentication response could be included in the handover execution as an additional message. More preferable the handover complete message could be extended or replaced by a modified authentication response as first contact of the MS to the new NAP. In this case the standardization needs to be changed a little bit. The modification is needed if the time saved by use of location data is shorter than the time needed to calculate the complete authentication. Then the time between handover command and the connection to the new network can be used to finish calculations. In a few cases the authentication will take even longer than this additional time, and then the MS has to inform the new NAP about successful handover but still lasting

authentication process. The messages need to be buffered until the authentication took place but the resources will remain reserved and the connection will not be lost but just delayed.

For the handover from GSM to Wi-Fi MS and NAP1 perform the GSM procedure (cf. fig. 1) and NAP2 and MS perform the 802.11 handover (cf. fig 2 a). This is how other handover procedures can also be implemented. NAP1 always performs a handover according to its protocol while NAP2 also uses its own protocol. But this may differ from the protocol from NAP1. The messages from NAP2 are tunneled and forwarded by NAP1 as encapsulated data. No message has to be translated as the MS is able to use both protocols involved. For its messages to the network the MS always uses the protocol associated with the actual air interface.

IV. Simulation Environment

The simulation area has a size of 50 x 50 km. The maximum number of cells inside this area is limited to 300. These cells belong to at minimum two different networks. The single networks differ in cell sizes and cell topologies (see an example in figure 4).

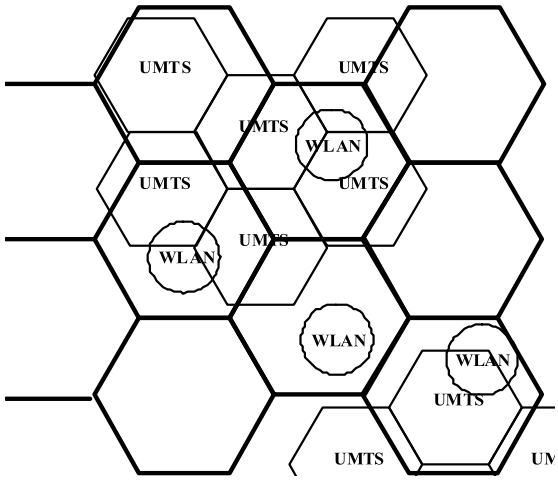

Fig. 4: Simulation scenario with underlying hexagon GSM network and islands of hexagon UMTS cells and single Wi-Fi cells (printed in circles for better distinguish ability). Overlap areas are omitted for better legibility.

But also different cell sizes in one network are considered to reflect different capacity needs in different places (rural/urban). This leads to a broad variety of overlap areas from very small to almost completely overlapping and from overlapping of two up to eight cells. (For an example of a detailed overlap structure in figure 5.) Therefore the results include some worst case constellations and can be assumed as realistic even with a non-optimal cell planning. GSM networks have been considered with cell sizes of 500 m, 2 km, 4 km, 7 km, 10 km, and 15 km, UMTS with 100 m, 500 m, 1 km, 2 km, 3 km, and 5 km and Wi-Fi with 50 m, 100 m and 300 m. Four different topologies are considered according to figure 6.

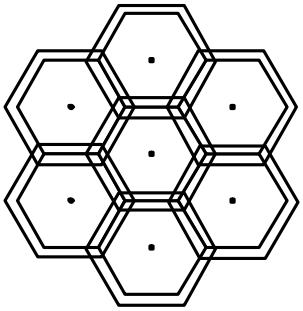

Fig. 5: Sketch of the overlap areas considered.

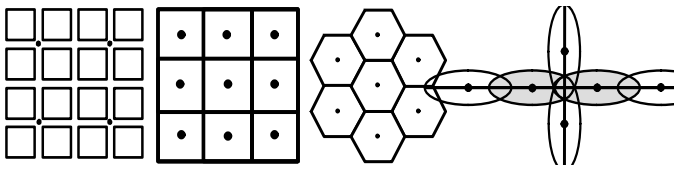

Fig. 6: Network topologies: from left to right Manhattan grid, square, hexagon, line network. Dots indicate the position of the network access point.

The hybrid networks for the 7200 simulations have been divided into six groups of 1200 simulations each: GSM⇔GSM, GSM⇔UMTS, UMTS⇔UMTS, GSM⇔Wi-Fi, UMTS⇔Wi-Fi and GSM⇔UMTS⇔Wi-Fi. In the single groups the cell sizes were distributed uniformly according to the values above. The sizes of the networks can be modified independently. For the simulations given here the network named first always had a cell size larger or equal to the second network. This is a realistic assumption as the networks are listed in order of increasing transmit frequency and therefore increasing attenuation in the propagation path.

Note that since Wi-Fi consists of comparatively small island networks it is not suited for fast users. That is why we only consider the handovers from Wi-Fi to other networks in the evaluation but not vice versa (although they are performed in the simulation, but have rarely been successful). These former handovers allow the users to stay connected if they leave the Wi-Fi islands. Handovers to Wi-Fi on the other hand are only reasonable if the user is slow enough. Otherwise even if the handover to Wi-Fi is successful it is doubtful if the successive handover back into another network will be executed in time. Users with a speed of more than 5 km/h should be prevented from handovers to Wi-Fi. Previous simulations have shown that users with a speed of more than 8 km/h do not manage two successful consecutive handovers with a reasonable rate. The rate drops below 30%. But also the first handover - to Wi-Fi - is only about 50% [14].

Besides the different topologies also different types of users are distinguished by different mobility models. Pedestrian users have a small velocity but may change speed and direction abruptly. The urban user is considered as driving in a car. He stops more often than the also driving rural user as it is assumed that there are more crossings, traffic lights and heavier traffic in the city. Therefore the urban user is also slower than his rural equivalent.

The appropriate mobility model is also reflected in the topology if network planning reflects the user density and expected data traffic needs. Not every model is suited for

every topology. In a first step the size of the area in which the user with the according model moves is restricted to the area that is covered by his home network plus about 20% overlap. That means a user with rural mobility model may penetrate into an area with urban topology but he is likely not to stay there very long as it is the boundary of his movement area. In further simulations the mobility models will be linked to the topology and change automatically to reflect longer periods of travel in different areas. Nevertheless there is still a considerable amount of movements that may be faster than the general speed of users in this topology. The intention of this overlap of mobility models in other areas reflects the chance of users not behaving as intended. On the other hand it also reflects the situation that quite often there are motorways or high-speed tracks crossing a city. Besides, Wi-Fi networks may also be reached by non-pedestrian users. Therefore in the simulation a certain amount of users has a speed which the network planning did not take into account. The assigned topologies of the (home) networks differ depending on the velocity of the user and the clutter class according to table II.

TABLE II
SIMULATION SCENARIOS.

Name	**Pedestrian**	**Urban**	**Rural**	**High speed**
Vmax	4 km/h	50 km/h	250 km/h	500 km/h
Mobility model	random walk [14]	vehicle-borne [15]	modified vehicle-borne [15, 13]	high-speed [13]
Topology	Manhattan Grid	Square, Hexagon	Square, Hexagon	Line, Line enhanced [13]

Vmax denotes the maximum velocity of the user.

The topologies and mobility models focused on urban environments as this is where handovers take place more frequently. Thus, 90% of the simulated hybrid networks contained at least one network with urban environment and therefore vehicle-borne mobility. The remaining 10% consisted of rural-rural or rural-high-speed scenarios. For the 90% urban scenarios, pedestrian and rural networks both have been included in 45% of the simulations while high-speed scenarios have been included in 20% of the scenarios. This results from the fact that there have been simulations with three different networks. These mainly consisted of different urban, rural or pedestrian scenarios, but in some cases the third network had high-speed topology.

The mobility patterns [14-16] are calculated in MatLab and then imported into ns-2. This allows the use of the same pattern in different network combinations, e.g. GSG-GSM or GSM-UMTS networks of the same topology category. With this approach the effect of the single protocols on the handover success can be investigated.

V. SIMULATION RESULTS

Our results show that the prior knowledge of the target cell and more efficient preparation for the handover can help to decrease the dropping rate especially for handovers between different networks and higher velocities. Table III shows percentages of successful handovers with different hybrid approaches. They are below 100% as there are capacity restrictions and the overlap with the best suited target cell may not be large enough to complete the handover successfully. Besides, sometimes the target cell is not predicted correctly as the measurement data may be insufficient in some cases.

TABLE III
SUCCESSFUL HANDOVERS.

Serving and target network	**Unmodified conventional handover without authentication**	**Hybrid handover with authentication before handover command**	**Hybrid handover with authentication after handover command**
GSM - GSM	98.87%	92.57%	96.37%
UMTS - UMTS	97.13%	90.69%	94.45%
GSM - UMTS	98.99%	98.37%	99.44%
UMTS - GSM	99.03%	99.21%	99.23%
Wi-Fi - GSM	No standard	77.95%	81.21%
Wi-Fi - UMTS	No standard	83.57%	87.20%

The conventional handover has a slightly higher success rate but it does not contain authentication. For comparison reasons the conventional handover has been modified by starting a complete authentication directly after the handover required message. As key conversion may have caused additional latency only intra GSM and intra UMTS have been simulated. As expected the handover success rate for the modified conventional handover dropped significantly to 29.45% in GSM and 27.67% in UMTS. Authentication only could be completed when the MS moved in the overlap area more or less parallel to the cell border for a longer period of time. Compared to the handover with authentication the location-based hybrid handover is about three times better in terms of successful completion within a given time.

The handover success rate of handovers from Wi-Fi to other networks is relatively small. This is because in the simulations we included waiting for a verifying measurement (scan). Therefore the measurements sometimes took more time than the overlap region allowed. Handovers from Wi-Fi anyway need to be supported by information about available networks. Otherwise the success rate will drop below 50% because the neighboring network only will be detected by chance if the right air interface is powered up in the overlap region and before leaving the Wi-Fi network. In the simulations all networks had information about the coexisting networks and only took measurements on the corresponding air interfaces, other networks have not been scanned, so other interfaces did not have to be powered up. This reduces the time needed.

The rate of successful handovers (including high-speed scenarios) is between 90 % and 99.5% for GSM and UMTS and between 77.9 % and 87.2% for handovers from Wi-Fi. The low rate for Wi-Fi of course depends on the fact that Wi-Fi is not designed for interoperation with the other networks. But in this simulation it also reflects the fact that Wi-Fi by far has the smallest cell sizes and thus the shortest available measurement times. If the cells of the other networks were as small and in an island topology their handovers would also be less successful. But for all networks it can be seen that the late authentication response significantly increases the success rate in most cases.

The simulations also have been used to determine the percentage of correct choices of the target cell. The right target cell here is assumed to be the cell that provides the highest

data rate at a given location. The success rate hereby depends on the velocity of the MS as well as on the cell size of serving and target cell. With the measurement data used in this simulation (RSSI only) over 90% of all GSM/UMTS handovers have chosen the right cell, for Wi-Fi this value drops between 53 and 85% [14].

In future investigations the utility function will be modified. The user should be allowed to define his preferences. Besides data rate quality of service, network provider, security features and others may be important for the user. For the operators it will be a selling argument to allow the private definition of a utility function by choosing between different options offered. Maybe the users will also be allowed to create own profiles by weighting the different preference categories.

VI. Conclusions and Outlook

We have proposed and evaluated a hybrid handover protocol that requires no or only very small changes in the existing standardization. With a subset of the specified measurements for GSM and UMTS we could derive the best target cell with a location-based approach in more than 90% of the cases. The early knowledge of the target cell allows early resource reservation and pre-routing between serving NAP and target NAP, even if the MS is not moving inside the overlap area of serving and target NAP. The early derivation of the target cell also enables us to integrate mandatory authentication with the target network before the handover has been executed. This enhances the security and lays the foundation for hybrid (inter-operator) handovers. The change of the underlying network with integrated authentication ensures that each single network maintains its security level and is not affected by weaker security levels of cooperating networks. For inter-operator handovers this is compulsory.

Simulations showed that the proposed handover with authentication is nearly as successful as the conventional handover without authentication. The missing authentication could also be included in intra-network handovers if the preparation phase is rearranged according to our proposal. Thus, the new handover not only deals with the challenges of hybrid networks but also enhances existing handover procedures.

The simulation scenario will be further developed. An automatic change of the mobility model according to the cell topology will provide even more realistic data. Future simulations will also make use of different utility functions where not only data rate but also other user preferences may play a role. This will allow the operators to implement new pricing policies.

Besides that we will go into more details of the timing in the backbone network to see if and when the backbone structure noticeably contributes to the handover latency. We will also focus on the timing and the absolute values of the handover duration. Therefore latency of the backbone network will be included for different backbone routing procedures. Additional networks as WiMAX and others will also be included in the hybrid handover protocol.

References

[1] GSM 03.09, *Handover procedures*, ETSI TC-SMG GSM Technical specification v7.0.0, August 1998.

[2] UMTS 23.009, *Handover procedures*, 3GPP Technical specification v6.4.0, March 2006.

[3] CDMA2000, *CDMA2000 Wireless IP Network Standard,* X.S0011-D v1.0, March 2006.

[4] ITU G.114, *One-way transmission time,* May 2003.

[5] K. Kastell, A. Fernandez-Pello, D. Perez, U. Meyer, R. Jakoby, *Performance advantage and use of a location based handover algorithm,* Proc. IEEE VTC-fall2004, pp. 2876-2883, September 2004.

[6] IEEE Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Standard 802.11. August 1999.

[7] A. Mishra, M. Shin, W. Arbaugh, *An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process.* ACM SIGCOMM Computer Communication Review, vol. 33 issue 2, pp. 93-102. April 2003.

[8] M. S. Gast, *802.11 Wireless Networks, the Definitive Guide.* O'Reilly & Associates, pp. 114-137. USA 2002.

[9] L. Chen, X. Cai, R. Sofia, Z. Huang, *A Cross-Layer Fast Handover Scheme for Mobile WiMAX,* Proc. IEEE VTC-fall2007, September 2007.

[10] W. Jiao, P. Jiang, Y. Ma, *Fast handover Scheme for Real-Time Applications in Mobile WiMAX,* Proc. ICC2007, June 2007.

[11] E. Barkan, E. Biham, and N. Keller, "Instant ciphertextonly cryptanalysis of GSM encrypted communication," in Advances in Cryptology - CRYPTO

[12] International Telecommunication Union. General Characteristics of International Telephone Connections and International Telephone Circuits. ITU-TG.114, 1988.

[13] K. Kastell, R. Jakoby, *Fast Handover with Integrated Authentication for Hybrid Networks,* Proc. IEEE VTC-fall2006, September 2006.

[14] K. Kastell, *Sichere, schnelle, ortsbasierte Handover in hybriden Netzen*, Ph.D. thesis, Technische Universität Darmstadt, Shaker-Verlag, July 2007.

[15] C. Bettstetter, *Smooth is Better than Sharp: A Random Mobility Model for Simulation of Wireless Networks*. Proc.ACM International Workshop on Modelling, Analysis and Simulation of Wireless and Mobile Systems, pp. 19-27, 2001.

[16] P. I. Bratanov, E. Bonek, *Mobility Model of Vehicle-Borne Terminals in Urban Cellular Systems*, Transactions on Vehicular Technology 52, no. 5, pp. 947-952, 2003.

Kira Alexandra Kastell was born in Rotenburg an der Fulda in 1975 has received diplomas in Electrical Engineering from Fachhochschule Frankfurt – University of Applied Sciences in 1998 and FernUniversität in Hagen – University of Distance Education in 2002 as well as diplomas in business administration and economics, both in 2004. She received her doctor's degree from Technische Universität Darmstadt in 2007.

From 1998 to 2002 she worked as a project engineer GSM-R with Mannesmann Arcor AG & Co. Then she got a scholarship from German research association DGF in the research training group "System integration for ubiquitous computing in information technology". From 2007 to 2009 she has been professor at Technische Fachhochschule Berlin – University of Applied Sciences. Now she is a professor at Fachhochschule Frankfurt – University of Applied Sciences. Her research interests are handover protocols and localization as well as hybrid networks and wireless transmission and propagation.

She is member of IEEE, VDE and of the editorial board of Frequenz - Journal of RF/Microwave Engineering, Photonics and Communications.