

SECURE HANDOVER PROCEDURES

Kira Kastell
Darmstadt University of Technology
Institute of Microwave Engineering
Merckstr. 25
64283 Darmstadt, Germany
Tel.: +49 6151 16 2862
Fax: +49 6151 16 4367
email: kastell@hf.tu-darmstadt.de

Ulrike Meyer
Darmstadt University of Technology
Department of Computer Science
Alexanderstr. 10
64283 Darmstadt, Germany
Tel.: +49 6151 16 5541
Fax: +49 6151 16 6036
email: umeyer@cdc.informatik.tu-
darmstadt.de

Rolf Jakoby
Darmstadt University of Technology,
Institute of Microwave Engineering,
Merckstr. 25,
64283 Darmstadt, Germany,
Tel.: +49 6151 16 2862
Fax: +49 6151 16 4367
email: jakoby@hf.tu-darmstadt.de

Abstract — This paper presents some security issues of handover procedures with an emphasis on hybrid and high velocity networks. It describes functional as well as informational security problems that occur during handover procedures and presents how predicting the next cell during a handover procedure can help to solve these problems.

A cell prediction is especially possible in track bounded wireless networks and in hybrid settings between a wide area and a local area network. If the cells of the local area network are much smaller than the cells of the overlaying wide area network, the next cell for a handover from the local area to the wide area network is even uniquely determined and a priori known.

1. Introduction

A trend in wireless networking is enabling interoperation between different wireless technologies. The standardization institutions of mobile phone networks as well as those of wireless local area networks are working in this area. They expect high benefits from combining the nearly ubiquitous availability of wide area wireless networks like GSM/GPRS or UMTS with the higher data rates of wireless local area technologies like the IEEE WLAN 802.11 or HIPERLAN [1], [2].

The tightest form of interoperation between different technologies is providing handover procedures between them. Handover procedures allow a user to seamlessly use services while changing from one underlying access technology to another. Therefore no user interaction is required during handovers, the rerouted connection is neither lost nor interrupted and in the ideal case the user doesn't even perceive the change of network access.

In homogeneous networks a handover results in a horizontal change of the currently serving access point or base station (BS) and a redirection of the traffic over the new point of network access. In heterogeneous networks the wireless interface on the mobile station (MS) changes additionally.

Handover procedures in homogeneous settings are an integral feature of mobile phone networks and they are already integrated into wireless LAN technologies and standardization is ongoing [3]. Several architectures for

heterogeneous handovers have been suggested for example in [4], [5] and [6].

Two different security aspects for handover procedures in homogeneous and heterogeneous scenarios are investigated in this paper. One is the functional security or safety, which basically guarantees that the handover procedure works well. The other notion of security is informational security, which refers mainly to data and location confidentiality, access control and data integrity.

Functional security deals with the question of how to guarantee the availability, reliability and maintainability for a handover procedure. It aims to protect from malfunctions that are not caused by malicious attackers.

These topics are still under investigation, because the handover requirements are more complex for high-speed movement and interworking of different networks. Some high-speed issues will be discussed in section 2. The approach to meet the requirements is to save transmission time during the preparation of the handover. Section 2.2 explains how time slots can be saved from knowledge of network topology.

Informational security deals with protection against malfunctions that are intentionally caused by a malicious attacker. The main security challenge during handover procedures is that the MS has to establish a secure channel with the new point of access. In GSM/GPRS, UMTS and in handovers between GSM and UMTS the secure channel is established by reusing the key material already used to secure the communication with the last point of access [7], [8]. Authentication is not applied during handovers in these technologies. Section 3.1 shows shortcomings of this approach.

In heterogeneous networks authentication becomes more essential as access control becomes more complex. In mobile phone networks all subscribers currently associated with the network are allowed to be handed over. In a hybrid handover between a private WLAN of a company and a public mobile phone network the access by handover has to be restrictable.

Section 3.2 describes in which phase of a handover procedure an authentication can be integrated. The prediction of the next cell during handovers can be used to save time slots to integrate strong authentication.

2. Functional Security

Capacity, field strength and maintainability are ensured by defining planning constraints and propagation models. The resulting network topology is the starting point for the reliability and availability problems dealt with in this paper.

Although the functional security in homogeneous settings of the current standards is satisfactory for standard applications there is a scenario that can cause problems even in GSM and is not yet well studied. Assume a MS moves with very high speed (≥ 250 km/h) during a handover procedure and the planning constraints in this environment lead to very small cells. As a result the MS stays in the cell only for such a short time that not enough measurement data can be gathered. This problem will be exemplified by investigating the handover procedure during Group Receive Mode (GRM) in GSM.

2.1. The high velocity problem

From the specifications [9] of GRM it is clear that during a group call the listening station behaves as in idle mode. Therefore the data measurement needed for handover preparation takes a long time, e.g. the MS attempts to decode parameters within 15 s. The calculation of the average of 5 measurement samples spread over 3 to 5 s also takes at least the 3 s, the BS identity code (BSIC) is decoded every 10 s and the Broadcast channel (BCCH) at least every 30 s.

Networks with high reliability and availability requirements and with subscribers moving at high speed lead to small cells with a length of 2 to 3 km, depending on provider and field strength requirements. This is because high-speed environment often results in tunnels and forest aisle with high attenuation to the signal. Thus a MS stays in the same cell for 28.8 s, 21.8 s and 14.4 s if it is moving at speeds of 250, 330 and 500 km/h respectively.

So in the worst case no measurement takes place, while the MS is visiting a certain cell. To prevent network failures, a stand-alone GSM modification is necessary. It should ensure high-speed handovers while minimally changing the measurement requirements. As a side effect it leads to savings of time that can be used for other signaling traffic.

2.2. Solving the high velocity problem by cell prediction

To get around the problem described above the handover procedure has to be accelerated. Predicting the next cell can do this. One way to do predict the next cell uses knowledge of network topology, location and direction of the movement of the subscriber.

Moving with high speed leads to a special pattern of movement. Subscribers move along lines, e.g. motorways and tracks. Therefore the shape of the planning area changes from area-wide to a line-shaped grid. This information can be used to perform handovers with nearly no measurement effort.

If subscribers move in one direction the next cell can be derived from knowledge of the network topology.

Considering Fig. 1, a MS coming from cell 1 will leave cell 2 towards cell 3. It is justifiable to leave aside turnarounds because of the high-speed movement. The next cell can easily be determined from the knowledge of the previous locations of the MS. In this ideal case each cell has only two neighbors.

At crossings there are two scenarios possible: A transmitter centered in the middle of the cell or two or more transmitters directing from the center of the crossing along the tracks. In both scenarios the direction of movement has to be predicted. The distance between MS and BS can be obtained from Timing Advance (TA) values. But for handover issues we also need information about the direction of movement.

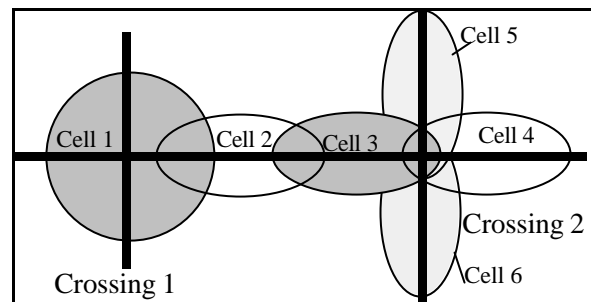


Fig. 1. Network topology of a line shaped network with two cellular patterns for crossings.

In line-shaped networks this direction can be derived by knowledge of the last serving cell. This information can be forwarded to the new serving cell during the handover procedure and the new serving cell can determine the cell for the next handover instantly.

If there are more target cells for handover the incoming direction information about the last cell is not sufficient. The current cell can ask the MS for more information. For measurement of the location of a MS there are several ideas discussed [10, 11, 12]. It is proposed to extract position data from TA measurement of three BSs with contact to the MS (3TA). In line-shaped networks two BSs are sufficient to derive location data, because of the knowledge, where the lines are (Fig. 2). This reduces the measurements for the MS.

In a line network, ideally there should be no contact to more than two BSs. In this case, incoming information can be used, because there is just one target cell, or the two cells TA mentioned above. If the MS reaches crossings the number of detected BSs increases and the 3TA measurement has to be used. If there are several crossings and changes of direction the speed will not be that high and the usual handover procedure can be applied.

In train environment or following a route-planning program for cars, handover information can also be taken from the schedule. Just the exact point of time for the handover performance has to be verified by observing TA data. The BS on its own can do this, so that the air interface can be used for other signaling events at the same time.

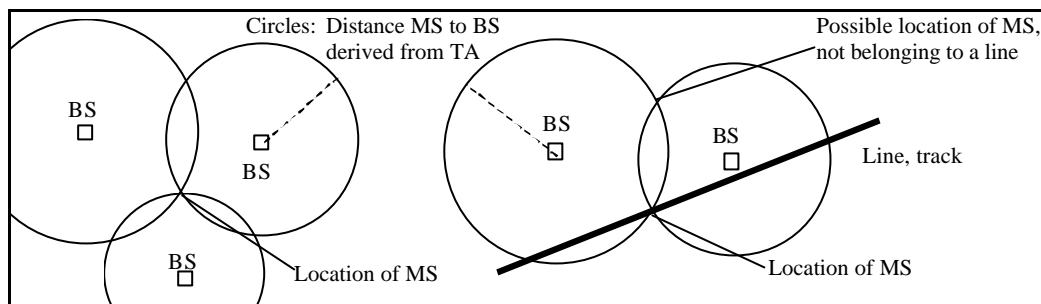


Fig. 2. Positioning with knowledge of the TA of a MS and tree surrounding BSs.

If the BS knows the direction and location of the MS in the network, it can either force the MS to perform a handover to the next cell at a certain point of time, depending on the speed of the subscriber or just to perform a handover to that cell, as soon as the MS detects that the field strength becomes to low. Beside the field strength measurement for the current BS and the TA measurement, no additional measures are required. The number of measurements of neighboring cells is reduced, the handover is accelerated and the functional security increased.

Another problem that may occur in high-speed line networks is an overlaying area-wide network. If both networks use the same channels and handover is allowed between them, then the overlaying serving cell of the area-wide network has more neighbors than the line network cell. It has to be ensured that the cell is only forwarded to line-compliant BSs. The BS of the area-wide network has to switch from normal to line handover to determine the right cell with the line prediction algorithms. In this scenario two different neighborhood lists may be used for each BS.

The next paragraph shows that heterogeneous networks and their applications pose new challenges with respect to access control and confidentiality during handover procedures. The integration of stronger security mechanisms in the handover process raises the signaling traffic between the MS and the network. Using the predicted handover technology described so far can save the amount of timeslot needed for this.

3. Informational Security in handover procedures

Whenever a MS connects to a point of network access it establishes a security context with a provider. During the handover process some or the entire network entities involved in the security mechanisms may change. Thus the current security context has to change as well. The MS and the network have to assure that they still communicate with each other and they have to agree upon the keys to use in the mechanisms applied to protect their communication. These mechanisms are an encryption algorithm and should include an integrity protection as well.

3.1. Shortcomings of some current standards

During handovers in networks like GSM/GPRS and UMTS no authentication is used [7], [8]. A MS that sends

on the expected channel and the expected time slot is taken as the MS for which the handover was initiated. This opens up handover procedures to a hijacking attack. An attacker can masquerade during the handover as the expected MS just by sending at the right frequency and time slot. As long as the attacker does not know the encryption and/or integrity keys currently used the attacker can not insert valid traffic into the channel and will therefore be detected not by the network but at least by the other end of the connection handed over. Nevertheless if an attacker can gain access to the key(s) e.g. because of a missing protection on the backbone network as described below he can impersonate the MS.

In voice applications session hijacking is not very interesting for an attacker. But it may course more serious concern in future. Hijacking a WAP session or a session from a user watching a video by streaming media technologies will certainly be more attractive.

The lack authentication leads to another problem that is highly relevant if we consider handovers in heterogeneous settings. This is the problem of granulating access control. For example in a handover between a private WLAN and UMTS not all of the UMTS subscribers should be handed over to WLAN. To distinguish between the MSs the respective provider has to authenticate the MS. A direct authentication during the handover procedure can protect against that and make the access control decision independent of the respective other provider.

On the other hand the MS has an interest to distinguish between different providers. E.g. the MS may want to permit or deny handovers dependent on pricing policies of the providers. A provider authentication enables this.

The accounting mechanisms of current standards are only designed for handovers within the network of one provider. A split during handovers is not provided. To enable handovers between different providers an authentication can be integrated.

In GSM/GPRS, UMTS and IEEE 802.11 WLAN a protection on the backbone network is not specified. Some recommendations are given, but unfortunately the communication between different entities in the network is often not encrypted and integrity protected. For example there are many GSM operators that do not protect the radio link between their fixed network and the BS. In GSM like in UMTS during a handover procedure the key(s) used to protect the traffic between the MS and the previous BS are reused to protect the traffic between the MS and the next BS. The key(s) are forwarded to the next BS and can be

- [6] Pahlavan, K. et al., "Handoff in Hybrid Mobile Data Networks", IEEE Pers. Commun., Apr. 2000.
- [7] ETSI, "Digital cellular telecommunications system (Phase 2+); Handover procedures", ETSI TS 100 527 V.7.0.0.
- [8] 3GPP, "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Handover requirements between UTRAN and GERAN or other radio systems", 3GPP TS 22.129 V5.2.0, Aug. 2002.
- [9] 3GPP, "Functions related to Mobile Station (MS) in idle mode and group receive mode", 3GPP TS 03.22 V8.7.0., Aug. 2002.
- [10] 3GPP, "Functional stage 2 description of Location Services (LCS) in GERAN", 3GPP TS 43.059 V6.1.0, June 2003.
- [11] 3GPP, "Stage 2 functional specification of User Equipment (UE) positioning in UTRAN", 3GPP TS 25.305 V5.6.0, June 2003.
- [12] Bartlett, D. et al., "CVB, A technique to improve OTDOA positioning in 3G networks", Cambridge Positioning Systems, May 2002 .
- [13] ETSI, "Digital cellular telecommunications system (Phase 2+); Performance requirements on the mobile radio interface", ETSI EN 300 944 V8.01, Aug. 2000.