WINES: a Wireless Network Simulator for Network Management Applications

Technical Report No RR 96 023

Didier Samfat and Christian Bonnet
Institut Eurécom
2229, route des Crêtes,
BP 193
06904 Sophia-Antipolis,
FRANCE
Tel (+33) 93.00.26.26 Fax (+33) 93.00.26.27
{samfat, bonnet}@eurecom.fr

Abstract - **In this paper we present WINES, a digital cellular network simulator which has been developed in accordance to the GSM technical specifications. The resulting platform is able to simulate the whole network as well as the mobile stations at the protocol level. The modular approach adopted for the GSM simulator functional architecture allow the network model portion of the program to be easily transported to various network applications. WINES is flexible as it was used to validate a generic intrusion detection architecture for mobile networks and integrated into a network planning tool. Other applications based on the layer-3 signalling analysis could easily be implemented with such a platform.**

Keywords: Simulation, protocols, GSM, intrusion detection, technical fraud, subscription fraud, network planning tool, trunk dimensioning, traffic forecast

1 Introduction

The Global System for Mobile communications (GSM) is being more and more popular and has prompted the design of many new network applications. Although GSM benefits from authentication mechanisms, they are inadequate confronted with malicious attacks such as the theft of the mobile unit, subscription fraud and network facility fraud[1] [10]. Therefore, one way to overcome these problems is to develop an Intrusion Detection System (IDS) which is a complementary approach to prevention based mechanisms [2]. The complexity of such IDS is growing in the case of Global System for Mobile (GSM) because in the near future, GSM will provide the same service in most European countries: a subscriber will have access to various network managed by different administrative authorities whilst retaining the same mobile unit.

In order to develop an IDS, a Wireless Network Simulator (WINES) becomes a mandatory requirement as existing networks are not always available to test the early IDS prototypes during the software development phases. Moreover, even if such networks were available, the provision of a wide range of traffic generators spread over a wide geographic area is costly and difficult to perform. These problems can be overcome by the use of simulators which also present the advantage of providing exact repetition of successive runs (useful during software implementation).

The growing success of GSM has stimulated operators to extend their networks. This cannot be achieved without a Network Planning Tool (NPT) whose purpose is to provide network service planning, prediction of resources allocation and analysis of the network behaviour during overloading. As the creation of an overloading situation cannot be envisioned in a real GSM network, the integration of WINES in the design of a NPT will allow network designers to perform an accurate forecast of future traffic and to re-dimension an existing network configuration for a given traffic load.

This is because of the aforementioned reasons that we have developed the GSM simulator WINES, allowing operators to view the system as a real implementation of the network. In Section 2, we briefly present the GSM architecture. Section 3 describes the simulation platform as well as the advantages of our approach. In Section 4 we illustrate the flexibility and the capabilities of WINES by presenting its utilization in two different mobile network applications: first, WINES allowed us to perform experiments for the validation of an IDS for mobile networks; second, this simulator has been easily modified in order to provide network designers an efficient tool for the planning of their GSM network.

2 GSM Architecture Overview

In the GSM architecture the whole network is referred as the Public Land Mobile Network (PLMN) which is composed of three parts with reference to Figure 1: the Mobile Station (MS), the Base Station Sub-system (BSS) and the Network Switching Sub-system (NSS) [1]. The MS has two components: the Mobile Equipment (ME) (the hardware equipment available from a dealer) and the Subscriber Identity Module (SIM) which is a smart card containing the subscriber's data. This allows the application of one of the principles of Personal Communications, as a call is not

1. *These frauds have already been encountered in GSM*

directed to a particular piece of hardware but to a subscriber who personalizes an MS by inserting his SIM into the ME.

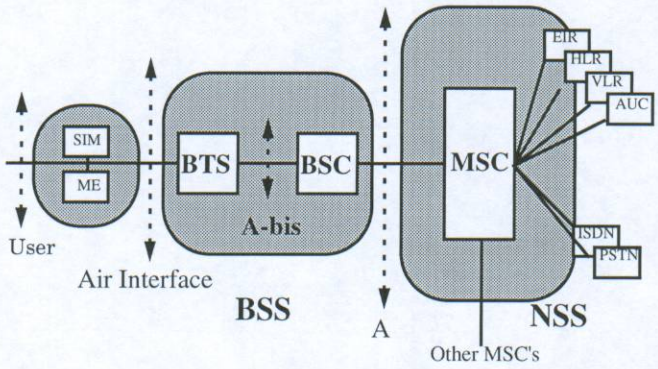

Figure 1 GSM System Architecture

The BSS is in charge of providing and managing transmission paths between the MS and the fixed network; it is composed of the following functional blocks:

- **Base Transceiver Station** (BTS). The BTS is the radio part of the fixed network, communicating with the mobile stations through the air interface and also performing measurements of the quality of radio communications.
- **Base Station Controller** (BSC). The BSC is in charge of radio resources allocation; it relays messages concerning call control and mobility management between the MSC and the MS, and also takes handover decisions according to measurement results.

The NSS performs switching functions and communications management functions in order to connect the MS to the desired destination networks or to an other MS. The NSS it is composed of the following entities:

- **Home Location Register** (HLR). The HLR is the main database of the system. It stores informations about the subscribers such as subscription type and current location.
- **Mobile Switching Centre** (MSC). The MSC is the switching centre of the network and manages the call control and the mobility aspects. It communicates with the HLR for the location updating procedures, with other MSCs for handover[1], and with the Gateway MSC for the routing of incoming calls. The Visitor Location Register (VLR) is a local database holding some of the information contained in the HLR concerning the MS managed by the current MSC.
- **Gateway MSC** (GMSC). The GMSC acts as a gateway for incoming calls and provides access to other PLMNs. When a call is directed to a subscriber of the PLMN, the GMSC questions the HLR about the current location of the MS and forwards the call to the respective MSC.

1. Changing of cell without interrupting the call

3 The Network Simulator

The GSM network simulator has been developed with OPNET software [17]. The resulting platform model simulates the BSS, the NSS and the MS as described in section 2. All layer-3 messages exchanged by the different GSM entities have been implemented in accordance with the GSM recommendation. The global architecture is depicted in Figure 2.

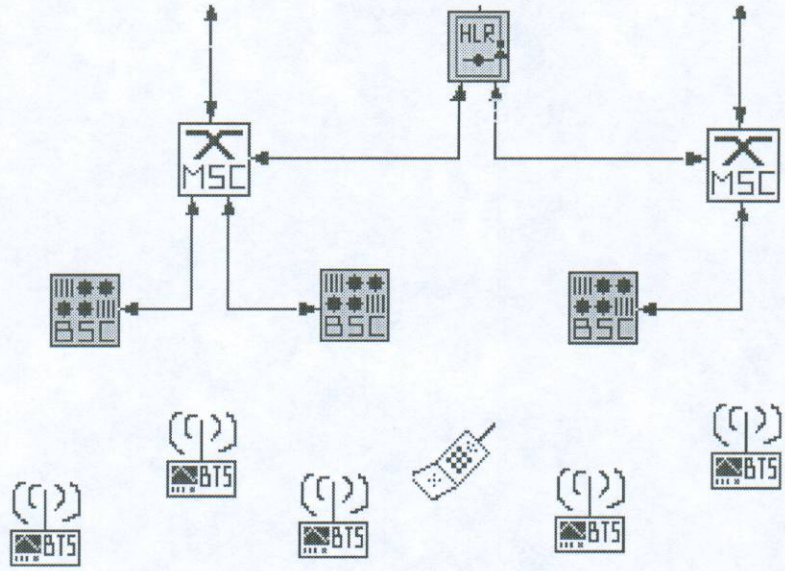

Figure 2 : A Portion of the basic version of WINES.

3.1 Design Approach for the NSS and the BSS

In addition to the basic requirement of designing a GSM simulator which is as close as possible to the real network, the following design criteria have been taken into account:

- **Portability**: Since the simulator has been programmed in C language it can run on different hardware/software architectures.
- **Scalability**: The platform is able to simulate a GSM network composed of several PLMNs. This requirement is important if we want to predict the behaviour of interconnected PLMNs.
- **Customizability**: Various GSM network topology can be created. For instance, a location area can be composed of one to several cells.
- **Flexibility**: Specific variables of the different entities and functions of the GSM simulator are easily adjustable by the use of parameters.

All GSM entities of the NSS and the BSS are OPNET network nodes; each network node is composed of one or several processors[1] and of several emitter-receiver pairs for the network connection. Furthermore, each processor is associated to a finite state machine (FSM) whose main function is to manage the different GSM protocols (RIL-3, MAP, BSSMAP) [15], [16]. In order to

1. *Depending on the complexity of the GSM component*

reduce the simulation time and test the platform for the intrusion detection architecture, all communications are assumed to be reliable[1].

A BTS has several attributes which help in defining the characteristics of the cell to be chosen upon a handover during the target cell selection procedure. Furthermore, a «beacon frequency» attribute may also be chosen for each BTS. The radio equipment of a BTS is connected to 5 links representing 4 dedicated channels and one common channel allowing simultaneous communications with the mobile stations.

A BSC manages a table of allocated channels where each entry in the table is a structure describing the availability, the connection identification with a BTS (or MSC) and the type of a channel.

A MSC has a connection table where each entry is also a structure describing the active connections and other informations relevant to the call control and handover processing. In the platform, the VLR is integrated to the MSC node as it is typically done in real GSM networks.

In addition to the GSM entities, two special nodes have been represented:

- The PSTN node (Public Switching Telephony Network) for the simulation of mobile originating and terminating calls.
- The SS7 node (Signalling System number 7) has been implemented in order to connect different public networks.

The SS7 protocols has been simplified[2] in order to reduce the simulation time. The main function of the SS7 node is to route signalling messages towards the NSS entities and the PSTN.

3.2 Implemented Procedures

The simulator is able to perform common procedures specific to cellular mobile networks. We briefly describe these procedures which require the participation of the different GSM entities.

Location updating (locup). This procedure is triggered by the MS each time its current location area changes. The corresponding information is sent by the BTSs on their control channel. The goal of this procedure is two folds: first, it allows the HLR to know which MSC is currently in charge of the MS, second, it registers the MS in the VLR of the current MSC. The location updating request emitted by the MS is processed by the new MSC:

- If the old location area was already under its control, an ***inter-BSC-locup*** procedure is performed and the MSC has only to update the VLR. However
- If the old and the new location areas are under the control of separate MSCs, an ***inter-MSC-locup*** is performed. In this case, the old MSC informs the HLR of the MS registration in the new VLR, as well as its entry cancellation in the old VLR.

---

1. *The loss of messages is not yet simulated*
2. *Only a light version of the Signalling Control Connection Part protocol and the Transaction Capabilities Application Part protocol have been implemented*

Mobile Originating call (MO). The mobile user can make a call towards the PSTN; the frequency and duration of these calls are parametrizable. The MSC relays the call request to the PSTN and establishes the connection [1].

Mobile Terminating call (MT). Calls can also be initiated by the PSTN which asks the Gateway MSC for routing information. Therefore, the GMSC asks the HLR for the roaming number provided by the current VLR and routes the call toward the current MSC. The MS is then paged in the location area where it was previously registered. Upon receipt of the reply from the MS, the MSC establishes the connection between the PSTN and the MS.

Handover. During a call, the BSC continuously analyses the measurement results sent by the BTS in order to decide on a potential handover. The following procedures are performed depending on the type of handover:

- ***internal-handover***: the MS moves from a current cell to a target cell both managed by the same BSC
- ***inter-BSC-handover:*** the MS moves to a target cell managed by another BSC in the same MSC area
- ***inter-MSC-handover:*** the MS moves from the anchor MSC[2] area toward a target cell in another MSC area (relay MSC area)
- ***subsequent-handover***: the MS moves from the relay MSC area to another relay MSC area, or is back to the anchor MSC area

3.3 The Mobile Station Model

In the basic version of the WINES a full implementation of the MS has been accomplished. The MS is a more complex node in contrast to the other GSM entities. At the network node level, various parameters such as trajectory, speed, altitude of the antenna for the radio-propagation can be set at simulation time; these parameters allows the definition of the propagation model. The MS requires the coordination of the following processors:

- USER-PROC represents the subscriber who is able to start or to end a call at any time.
- SIM-PROC reads and writes data on the SIM card.
- RACCH-PROC performs the access procedure of the MS and controls the emission of messages on the random access channel
- MC-PROC allows the MS to measure the quality of the reception. Upon receiving the corresponding results from the MS, the BSC is able to decide whether or not to perform handover and choose the best cell for the MS
- RE-PROC: The radio equipment is composed of an antenna with an isotropic pattern of a pair of transmitter/receiver

---

1. Speech data traffic is not yet simulated
2. MSC managing the MS at the beginning of the call

In addition, 4 other processors have been integrated to the MS model in order to manage the following protocol layers:

- RR-PROC: Radio Resource (RR) [13] is the sub-layer which manages the radio connection. RR protocol consists in establishing (or re-establishing) a dedicated channel when changing cells.
- MM-PROC: Mobility Management (MM) [14] is the sub-layer which performs the location update procedure. The security functions have not been implemented.
- CC-PROC: Call Control (CC) [12] is the sub-layer which manages the call performed by the mobile.
- PL-PROC: the physical layer process LAPDm messages[1][12].

Therefore, 9 FSMs are needed to ensure the inter-operability of the 9 MS processors which is able to handle up to 7 different cells simultaneously. Every packet arriving from the radio system is first processed by the measure computation FSM and is sent to the physical layer FSM which forwards CC, MM and RR messages to the corresponding FSM.

Additional parameters such as call frequency and call duration, allow the definition of the mobile user behaviour.

This model allows the analysis of the exact volume of signalling traffic generated on the radio path and in the network by one MS (with a particular customer activity as described in Table 1). depending on different scenario. Each scenario takes into account a combination of criteria such as synchronous/non-synchronous handover, location update and MT/MO calls. Moreover, we are able to vary the propagation conditions of the radio environment and thus to analyse the behaviour of the MS under such situations.

3.4 Mobile Station Generators

The complexity of the mobile station model forbids its duplication for the simulation of a wide network traffic because such approach requires a simulation time of several days. Network management applications such as intrusion detection and network planning which are essentially based on the analysis of the NSS traffic (see Section 4.1 and Section 4.2) do not require the simulation of the radio part.

Therefore, WINES has been modified in order to reduce computation time. In doing so, we made the design of a Mobile Station Generator (MS-GEN) which does not use the radio part. Only the protocols involving the BSC and the NSS entities which manage the telephony activity and the migration of mobile stations are simulated.

The goal of a MS-GEN is to simulate a population of mobile stations in order to generate realistic signalling and user data traffic within WINES. The characteristics of the generated traffic must be as closed as possible to the real traffic for a given GSM topology. Therefore, each MS-GEN is

1. *LAPDm is the only layer-2 protocol which has been implemented since layer 2 and 3 are both present in the SABM message.*

configured in order to activate a particular category of real GSM subscribers[1] as described in Table 1.

Type of User	DOMESTIC	CORPORATE	LOCAL BUSINESS	ROAMER
Daily Usage [a]	**10-15**	30-40	15-20	30 +
Calls per Week	12-16	20-25	12-15	25 +
National Call	95%	75%	99%	95%
International Call	5%	25%	1%	5%
Average Duration[b]	< 5	10	< 10	10 +
Call Time	Off peak	Peak Time	business Hours	Any
Destination Call	Mostly local	Nation Wide	Local	International
Origine of Call	Home Cell	Any MSC/BSC	Same MSC	All
Type of Call	MTL[c]	MTL and **MTM**[d]	MTL	MTL and MTM

Table 1 : Classification of GSM subscribers

a. Value in minutes
b. Value in minutes
c. Mobile to Land
d. Mobile to Mobile

Each MS-GEN is able to simulate a group of 1000 mobile stations with the same behaviour. The frequency and the duration of MO calls are parametrizable and the peak hours (busy period during the day) can also be defined. For each user, a scenario of behaviour is preestablished at the beginning of the simulation depending on the following statistical distributions:

- Duration of calls follows an exponential distribution
- Arrival of calls follows a poissonian distribution

These assumptions have been shown to be reasonably accurate for mobile telephone networks. In addition to the telephony activity, the parameters corresponding to the mobility of users can be defined:

- Number of handovers per call
- Number of location updates
- Number of location areas traversed

A simulation run can represent the behaviour of the network during one day. Therefore, a MS_GEN is able to simulate a population of MSs during work days or week-ends. The different MS-GENs can be run in parallel or in sequence:

- The parallel mode allows the network designer to obtain at the end of the simulation, relevant information about the behaviour of the GSM network during the day.

---

1. This classification of GSM subscribers was obtained from a french operator

- The sequential mode allows the analysis of the variation of the network load in an incremental way. For instance, it is possible for the network designer to measure the impact of an additional ten thousand MSs on the network for a given GSM topology.

The MS-GEN has been designed in order to be independant of the underlying simulated network and can be used for the generation of traffic in other wireless network simulator. However, using a MS-GEN requires that the normal BTSs be replaced by a derived entity called BTS-bis which translates mobile units activity[1] in terms of signalling messages. However, like a normal BTS a BTS-bis is conneted to a BSC via the A-bis interface. Moreover, each BTS-bis manages a connection table and routes messages between the BSC and the MS-GEN in charge of the current mobile station.

4 Network Management Applications Using WINES

The GSM platform has been implemented in order to test an intrusion detection system and to integrate a network planning tool. The reasons for such a choice are twofold. Firstly, the GSM network does not provide intrusion detection services to operators while ***subscription fraud*** and ***network facility fraud*** have already been encountered in GSM. Secondly, configuration, accounting and fault management functions are present in various management environments in contrast to performance and network planning functions which are more difficult to implement as they require data collection and thus create computational overhead.

4.1 Validation of an Intrusion Detection Architecture

WINES has been used to test and validate an Intrusion Detection Architecture for Mobile Networks (IDAMN). IDAMN is a distributed system whose main function is to track and detect mobile intruders in real-time. IDAMN includes two algorithms which model the behaviour of users in terms of both *telephony* activity and *migration* pattern. The main innovation of this architecture is its ability to perform intrusion detection in the visited location and within the duration of a typical call, as opposed to existing designs that require the reporting of all call data to the home location in order to perform the actual detection [14], [15]. The algorithms as well as the components of IDAMN have been designed in order to minimize the overhead incurred in the fixed part of the GSM network

IDAMN is functionally composed of two distinct entities: a Global Monitor (GM) and an Intrusion Detector (ID (both components have also been programmed with OPNET).

The main purpose of the GM is to manage and save over a long period the profiles of the subscribers normal behaviour. The ID is directly connected to the anchor[2] MSC and makes a copy of the relevant signalling messages generated by each mobile unit. Depending on the nature of the messages, the ID initializes a set of statistical variables and requests the GM the activity and mobility profiles as well as the global report concerning the mobile user. Then, the ID is able to detect a potential intrusion by comparing the variables to the profiles.

---

1. *A MS-GEN generates locup, handover an MO/MT calls events which must be transformed into the corresponding signalling protocol that the target simulator can understand*
2. *In GSM terminology, this is an MSC managing the MS at the beginning of a call*

The GM is able to access the HLR via the GSM standard protocol MAP/C in contrast to the ID which can retrieve information from the VLR using the MAP/B protocol [16]. Furthermore, a single ID is associated with each MSC allowing IDAMN to have a complete view on the mobile user in order to analyse his ***telephony activity*** and his ***migration pattern***.

The telephony activity of a mobile user is defined by two statistical vectors which are initialized by the ID upon receiving signalling messages from the anchor MSC. These statistical vectors are the following:

1. ***The Call Vector*** is a local magnitude which models the outgoing calls. In other words, each time a mobile user makes a call, the ID computes a statistical call vector over the frequency and duration of an outgoing call, number of handovers performed, time and duration of activation of the MS.
2. ***The Session Vector*** is a global magnitude which models the session behaviour of the user in terms network connection duration, total number of calls, total duration of calls and the total number of handovers

The values of both Call Vector and Session Vector are obtained when the anchor MSC performs the following procedures: *mo-call-start/stop, imsi-attach/detach, msc/bsc-locup* and *internal/ inter-BSC/inter-MSC/subsequent-handover*. In addition to the telephony activity analysis, the study of the ***migration pattern*** of each mobile users is performed. It allows us to analyse the mobility area of a subscriber as well as the most frequent paths used. A mobility behaviour profile based on a graph model (with probability transitions) is established depending on the frequency of location area crossings of the mobile user. This mobility profile is updated when the following procedures are performed: *inter-MSC-locup, inter-BSC-locup.*

Intrusions alarms are raised when the detector notices a strong variation of the mobile user behaviour compared to the mobility and activity profiles. These alarms are then analysed by a rule based system which gives the final decision.

4.2 Integration of WINES into a Network Planning Tool

Simulators based on WINES approach are of interests to operators because they can address two different needs at the same time:

- Replay of realistic scenarios based on accurate observations made on a real network in order to find the best configuration
- Experiment of hypothetical growing traffic in order to predict the ressources to be added to the existing network

Therefore, WINES has been integrated into a basic network planning tool in order to allow GSM operators to design the future extension of their BSS and NSS. The basic NPT is depicted in Figure 3 and is composed of several[1] MS-GEN, WINES (for the simulation of the BSS and NSS of GSM) and of an analysis tool which presents the output results in the form of histograms or graphs.

---

1. depending on the number of mobile stations to be simulated

Data are collected from a real GSM network and must be formatted in order to initiate the different MS-GEN variables as well as the parameters of statistical laws as mentioned in Section 3.4. Then, each MS-GEN activates a set of mobile stations which generate signalling messages in both BSS and NSS.

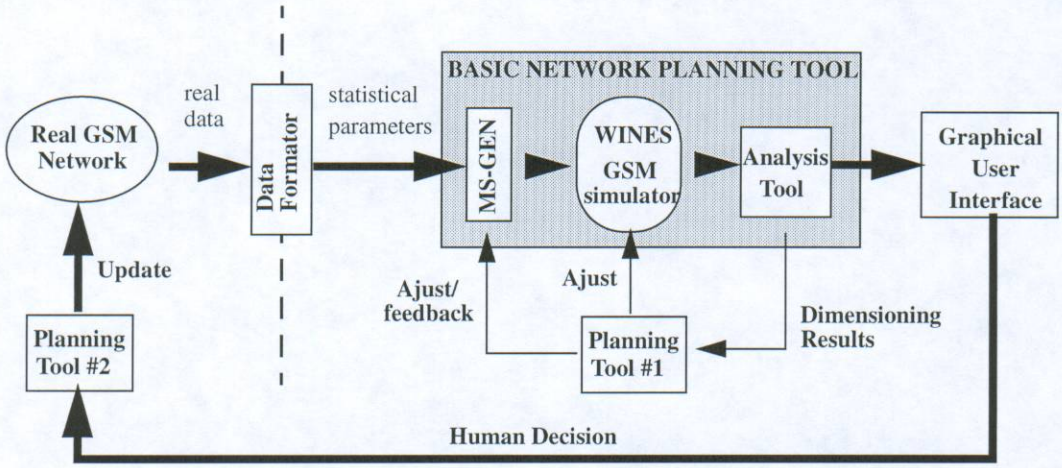

Figure 3 : Overview of a Network Planning Tool for GSM

In order to design an efficient planning tool, we have given WINES a set of new functions for the analysis of the generated traffic. These functions can help operators to assess the following network planning criteria:

- ***Traffic forecast***: WINES is able to perform an accurate prediction of future traffic on the basis of input parameters of the MS-GEN.
- ***Trunk dimensioning***: spy functions and probes located in the different BSC and MSC allow the conversion of point-to-point traffic load into trunk requirements. In other word, at the end of a simulation it is possible to determine the number of trunks needed to handle a simulated traffic.
- ***Equipment dimensioning***: for a given user population, it is possible to count the number of requests to the HLR as well as to the VLR and hence deduce the signalling transfer processing for these GSM entities.
- ***Common channel signalling dimensioning***: as we are able to dimension each signalling link at each interface[1]. As all signalling protocols have been implemented, it is possible to determine the occupancy of each link and to notice the capacity limits for a given population of mobile users.

In addition, three types of probes (or spy-functions) have been implemented at different levels of the GSM network: BTS, BSC and MSC nodes. These probes updates local statistics for each entity of the network; for instance, we are able to collect the following relevant information:

---

1. For instance the data rate

- Instantaneous traffic load in terms of dedicated channels such as Traffic Channel at Full rate (TCH/F) and Standalone Dedicated Control Channel (SDCCH)
- Number of handovers performed (or failed) by a specific entity in the network
- Number of location updates performed (or failed) at different levels of the network

Therefore, we can measure the number of TCHs and SDCCHs allocated to each BSC and MSC composing the simulated GSM network. In other words, we are able to represent the load variation on each link (in terms of number of dedicated channel manage by each entity) as a function of time.

With respect to the simulated traffic, it is also possible to measure the number of call requests failed due to the unavailability of radio channel resources within a cell. Moreover, the cell (namely a BTS) which rejected handovers or call requests can be identified. In a more general way, we are able to have an accurate overview of the simulated network during an overloading or a congestion situation.

At the end of a simulation, a graphical user interface displays the values of trunks dimensioning as well the number of dedicated channels needed for each GSM entity in order to manage the simulated traffic. Statistical results in the form of histograms and graphs representing the evolution in time of the switch capacity, the number of activated MS, and the traffic load of a specific GSM entity are also provided.

5 Summary

In conclusion, this paper presents a new modular approach to the simulation of mobile networks. WINES is the resulting platform which is able to simulate entire GSM network as well as the mobile stations at the layer-3 protocol level. Various GSM network topologies (including the NSS and BSS) can be created and different components (mobile stations and mobile stations generators) are available for the generation of traffic at the MS level or the NSS level. The mobile station generators have been designed to be independant of the simulated network and can be used in other mobile network simulators.

We showed that WINES can be of interest to network designers who can replay realistic scenarios based on observations made on a real network in order to find the best configuration for their GSM network. Moreover, the inherent flexibility of WINES allowed us to develop a network planing tool for GSM and to validate an intrusion detection architecture for mobile networks.

Future work includes an enhancement of WINES in order to take into account supplementary services such as short messages service, voice mail and facsimile. The objectives will be to provide an accurate analysis on the impact of the introduction of a new service to an existing GSM network.

6 References

[1] M. Mouly, M.B. Pautet, The GSM System for Mobile Communications, ISBN 2-9507190-0-7, 1993

[2] B. Mukherjee, L.T. Herbelein, K.N. Levitt, Network Intrusion Detection, IEEE Network Magazine, May/June 1994, VOL. 8 No 3.

[3] D. Samfat, V. Devernay, C. Bonnet, «A GSM Simulation Platform for Intrusion Detection», Proceedings of ICC'95, Seatle, June 1995

[4] Theresa F. Lunt, "IDES: An Intelligent System for Detecting Intruders", Proceedings of the Symposium: Computer Security, Threat and Countermeasures, Rome, Italy, November 1990.

[5] Rob Mechaley and Kirk Calson, «Parameters for Fraud Management Using Network Based Techniques», Technical Report 45.2.II.2, Mc Caw Cellular Communications, Inc, 1991

[6] Evan J. Davies, Henrik Nordin, Sharon Hershon, Kathy Gallup, «Design Overview for Fraud Detection and Analysis System», Technical Report, Digital Equipment Corporation, August 1992.

[7] GSM Recommendation 3.05, Signalling Requirements Relating to Routing of calls to Mobile Subscribers, ETSI Standard, Feb. 1992

[8] GSM Recommendation 3.09, Handover Procedures, ETSI Standard, Feb. 1992

[9] GSM Recommendation 3.12, Location Registration Procedures, ETSI Standard, Feb. 1992

[10] GSM Recommendation 4.08, Mobile Radio Interface Layer-3 Specification, ETSI Standard, Feb. 1992

[11] GSM Recommendation 9.02, MAP Specification, ETSI Standard, Feb. 1992

[12] GSM Recommendation 4.06, MS-BSS Data Link Layer Specification, ETSI Standard, Feb. 1992

[13] OPNET Network Simulation Software, MIL 3, Inc. 3400 International Drive, Washigton, DC 20008, Release 2.4.A