Selective Mobile Communication in Socially Sensitive Environments

Hatim M. Behairy · Waleed S. Alrobian · Adnan A. Alghammas ·
Brian R. Suter

Published online: 22 March 2014

© The Author(s) 2014. This article is published with open access at Springerlink.com

Abstract In certain environments, the use of mobile phones must be curtailed for the sake of security or out of respect for others. We present a novel method for selectively controlling mobile phone services in such areas using a base station controller and a sequence of detection steps to identify when the mobile device is within the coverage area. A prototype for the method has been developed using commercial off-the-shelf and custom designed hardware and software subsystems. Key components in the prototype system are two directional antennas located at the entry to the controlled area with one antenna facing outwards and the other inwards. By using the proposed detection method, the base station controller is able to detect when a mobile station enters or leaves the controlled area. Experiments using a variety of detection sequences by the two directional antennas and associated white- and blacklists of allowable and disallowed devices, respectively, confirm that the prototype system is able to effectively control the use of mobile devices within the coverage area.

Keywords GSM · Mobile communication · Sensitive environments

1 Introduction

The use of mobile devices has increased tremendously over the last decade. Today almost everybody carries a mobile device of some sort, whether a phone, a personal digital assistant

H. M. Behairy (✉) · W. S. Alrobian · A. A. Alghammas
National Electronics, Communications and Photonics Center, King Abdulaziz City
for Science and Technology, 6086, Riyadh 11442, Saudi Arabia
e-mail: hbehairy@kacst.edu.sa

W. S. Alrobian
e-mail: alrobian@kacst.edu.sa

A. A. Alghammas
e-mail: aalghammas@kacst.edu.sa

B. R. Suter
Tellumat Pty (LTD), Cape Town, South Africa
e-mail: bsuter@tellumat.com

(PDA), or a laptop. Because such devices have become such an integral part of our everyday lives, we carry them everywhere. In addition to the technical challenges from the increased usage of mobile devices—including spectrum optimization and radiation management—security, social, and etiquette complexities have arisen in areas where complete silence is expected or even mandated such as in schools, universities, places of worship, hospitals, and jails. In some environments, such as business meetings, places of worship, and hospitals, the use of mobile phones may be controlled out of respect. Moreover, in security sensitive areas control of mobile phones is critical and must be handled according to the security plan [1].

There are several reasons for controlling mobile communications in specific areas [2]. Using cell phones in certain situations may violate the rules of an establishment and threaten the integrity of the environment. For example, in a prison, organized crime could continue to run their organizations through the use of cellular phones. Preserving privacy is another reason to institute such control. In other situations, mobile phone usage may not fit the environment and proprietors of such a space would attempt to control this usage within their domain, e.g., a place of worship where cellular phones would disrupt prayers. Extensive usage of mobile phones by workers/employees lowers productivity resulting in increased costs and/or reduced revenues for the employer; e.g., the cost to an employer of employees spending many minutes on the phone for personal purposes could easily result in more than a man-week per year of lost productivity. Using cell phones in certain specific areas can be dangerous and pose safety risks, e.g., disrupting a calm peaceful environment in hospitals. Prohibition of mobile phone usage may also be necessary to protect the confidential nature of a building and the people, products, and documents therein, or to preserve the integrity of the institution, e.g., providing security for a business conference, board of directors' meeting, or seminar.

In this paper, we present a novel system for selectively controlling mobile phone services in desired controlled areas, which we call Class of Service Controlled Areas (CoSCAs) [3,4]. The selected mobile service (voice call, SMS, data) can be controlled in both directions (incoming and outgoing) and may be based on the identity of the user in a white/black list arrangement, where a whitelist is defined as a list of Mobile Stations (MSs) that are allowed certain services, while a blacklist is the list of MSs that are denied certain services in specific time of the day (during scheduled prayer times in a place of worship, for example), or simply the location, like a meeting room.

The remainder of this paper is organized as follows: In Sect. 2 typical methods that have been previously considered to resolve the problem are reviewed. In Sect. 3 the proposed system architecture is presented. In Sect. 4, the system prototype and empirical results are presented, while in Sect. 5 conclusion is given. Finally, in Sect. 6 further work is described.

2 Related Methods

Albeit the several methods that have been proposed in the literature to address the problem of silencing mobile phones including the review provided in [5], no practical solution has been proposed and implemented that does not require changes either at the network level or at the MS level.

In existing mobile communication networks, control of mobile devices can be achieved in many different ways with various effectiveness levels including cooperative control where the user of the mobile device willingly activates/deactivates features on the phone according to the regulations or recommendations for their current environment, such as switching the phone to silent mode if in a place of worship or even turning it completely off when in a

hospital or airplane. This requires the complete cooperation of the user, something that cannot be guaranteed in most cases.

The Mobile Network Operator (MNO) can at all times control any service on any segment in its network. However, this method is limited in that to control a certain area (which we call the controlled area) all MNOs must cooperate and apply control to that area, which does not give the keeper of the controlled area any flexibility in applying such control. From the MNO's point of view, this must of course be supported by an adequate business model (through some subscription model) because disabling a service for whatever reason in an area in which the MNO has invested in, may not be that appealing after all.

Another method of control is by shielding where a Faraday cage or Faraday shield [6]—which is an enclosure formed by conducting material or by a mesh of such material that blocks out external non static electric fields¹—effectively blocks all wireless signals in a specific area. However, because the cost of such a solution is much greater than the benefit derived from it, in practice, this solution is implemented in a very limited way.

Most common amongst all is the use of jammers. A jammer works by transmitting a noise signal at the same frequency as that at which the mobile devices operate [7]. This method gives the keeper of the controlled area the flexibility to disrupt all communications provided by any MNO whenever they need to. However, in addition to known jamming drawbacks, this method also terminates all services and renders the device out of order as long as it is within the range of the jammer's coverage, which is, after all, the essence of jamming. Of course, this completely disrupts all communication to and from the device, which means that no one can make or receive calls or use any other services even in an emergency situation. Additionally, in order to cover all the wireless mobile services such as GSM 900, GSM 1800, and 3G (UMTS) from all MNOs, the jammer needs to operate at all the related frequencies [7]. Moreover, because the base station's signal power in the desired area of control varies over time and is not precisely known most of the time, the jammer must be set to output a great deal of power to be certain to overpower the base station's signal. Another severe drawback of jamming is its negative impact on humans including potential health risks or interference with devices like pacemakers.

In [8], a method of non-intrusive control of a mobile device is described that provides for the remote control of an auditory volume and ringer sound level associated with a mobile device, dependent upon the location of the device. A set of location-dependent rules are established and stored in a database. The location of the mobile device is determined and compared to the location-dependent rules in the database. A control signal is transmitted by the wireless mobile network to the mobile device to adjust the ringer sound level and/or auditory volume of the device. Alternatively, the mobile device may be programmed with a user consent routine, requiring the user to provide consent before the control signal may adjust the volume. If the ringer sound level is set to Zero, the user's subsequent messages may be automatically rerouted to a voicemail system.

In [9], a method for suppressing ring tones in cellular telephones and for informing a cellular telephone with configuration data is described. The method includes detecting a cellular telephone that enters a space time zone associated with the network. A property of the telephone is determined. Information is sent to the telephone that relates to the telephone property and a characteristic of the network space time zone.

In [10], a method is presented where a mobile terminal receives a device identifier from a Short Distance Communication (SDC) device located near the area where the mobile terminal is to be controlled by using the internal SDC device disposed in the mobile terminal. The

¹ www.wikipedia.com.

mobile terminal will then determine whether the received device identifier corresponds to or includes one of identifiers stored in the mobile terminal and if so, the mobile terminal performs a predetermined control function corresponding to the identifier.

In both [8] and [9] the scope was limited to suppressing the ring tones and no attempt was done to control the service provided to the cellular phone based on space time zone, the subject of this paper. In [10], a control program must be included in the mobile terminal for it to communicate with the SDC device and determine the appropriate control. This of course requires the cooperation of the mobile terminal user and that the device is previously known and loaded with the control program.

3 Proposed System Architecture

To control a specific area (CoSCA), we propose a system consisting of two virtual Base Transceiver Stations (vBTSs), each connected to a directional antenna. A directional transmit/receive (TRX) antenna is connected on each side of a single doorway (Locating Access and Control Point, LACP) to monitor and report on a Mobile Station (MS) entering and/or leaving the entrance doorway controlling access to the CoSCA as shown in Fig. 1, where the vBTS units are represented by “MSCoS BTS/BSC” entity which is set up, as described, to clone GSM BTS within the MNO and using controlled power. The first antenna points outwards of the controlled area (outer antenna), while the other points inwards in the controlled area (inner antenna). The motivation behind this design is to detect an MS identity when passing through the gate of the CoSCA by triggering a sequence of events. If an MS is detected first by the outer antenna and then by the inner antenna, it is considered to be within the CoSCA. This does not include those cases where an MS happens to be physically located within the CoSCA, and does not trigger the two antennas in the sequence prescribed earlier. For an MS to be considered controlled, it has to be within the CoSCA and respond to paging signals from the inner antenna. If an MS, which is already controlled, is detected

Fig. 1 Architectural features of the system

by the outer antenna, it is eligible to be released or uncontrolled. The two vBTSs are hosted in the CoSCA and are connected to the antennas using radio frequency (RF) cables.

In the overall system configuration, a CoSCA is defined by two local vBTSs and their associated antennas and one local base station controller (BSC). A CoSCA is connected to a Central Management Server (CMS) through a TCP/IP connection. The CMS connects to all CoSCAs deployed in a number of different locations. The CMS receives all MS data collected from each CoSCA for which a black/white list is defined. In the CMS, the MS data received from a CoSCA, which is the International Mobile Equipment Identity (IMEI) and International Mobile Subscriber Identity (IMSI), are checked against the black/white list for the particular CoSCA to determine whether to control the MS.

To force an MS passing through the gate of a CoSCA to connect to the two vBTSs installed at the CoSCA gate, a signal stronger than that to which the MS is connected is broadcast through the two antennas. This will attract the MS to connect to the vBTS with the stronger signal, which in turn will force the MS to transmit its (IMEI, IMSI) information to identify itself and camp to the local vBTS. The vBTS will then be able to collect the data and pass it through the BSC to the CMS server for verification and decision making.

The system can be operated in two different modes. In the first mode (local mode) no external connections to the MNOs are necessary. Control of the CoSCA is achieved by keeping the MS connected to the local vBTS at the CoSCA and not providing any of the MNO services if the MS is not on the white list of allowed MSs. On the other hand, if an MS is on the white list, the local vBTS at the CoSCA will release the MS by denying its request for connecting. In this way the MS will reconnect to the MNO BTS and continue functioning as normal.

In the other mode of operation (connected mode), the details provided to the CMS are available for use by the MNO (or a third party). All the decisions to control/release an MS are done by the MNO. The MNOs, through business agreements with the keepers of a CoSCA, can allow/disallow certain services based on a particular attribute to provide or not to provide certain services (voice or data, for example) to selected MSs according to the white list, time of day, or location. The MNO will then need to integrate an additional step in its paging process to include a check whether the MS to be paged is under control for those particular services. In this paper, we will restrict our discussion to cover the first mode (local mode) of operation.

In both modes of operation, coordination with the spectrum authorities in the country and MNOs to operate this system is necessary. The proposed system, including vBTS must not in any way interfere with MNO services in other locations. Therefore, tight control on the transmitted power out of the vBTSs and antennas used must be applied, making sure they do not spill over out of the intended coverage area (CoSCA). It is also crucial that only legitimate keepers of areas with prior coordination with the designated authorities can install such devices for security reasons.

Typically, an MS connects to the strongest BTS in its vicinity, and to get the MS to connect to the vBTS we need to mimic a valid BTS. To do so, a radio survey must be conducted in the desired area to be controlled to measure the RF levels and other parameters that will be used. Each BTS broadcasts on one or more fixed Absolute Radio Frequency Channel Numbers (ARFCNs). The following Broadcast Control Channel (BCCH) parameters are monitored during the measurement: BCCH Allocation (BA) list, Location Area Code (LAC), Cell Reselection Offset (CRO) value, the Cell Reselect Hysteresis (CRH) value, the Calculated Cell reselection (C2) value, Mobile Network Code (MNC), Mobile Country Code (MCC), Network Color Code (NCC), Cell ID (CID), and Base Station Identity Code (BSIC). These values are received in System Information (SI) messages that are broadcast periodically on

the BCCH by the various BTS. The mobile device is only allowed to attach to a BTS that meets three conditions:

1. The BTS must be the highest-ranked signal measured by comparing C2 levels of the current serving cell and the C2 of all candidate serving cells. The C2 value is calculated by adding the received power level (Rx) to the optional Cell Reselection Offset (CRO) power parameter. Thus the CRO of the vBTS can be used to cause a virtual increase in power. This can be expressed as: $C2 = (C1 + CRO)$ (where C1 is equal to $RxLev - RXLEV_ACCESSMIN$ a fixed constant dB offset) [11].
2. The mobile device will only take into account the C2 value of any candidate serving cell where the candidate serving cell ARFCN is in the BA list (BCCH Allocation list) received from its current serving cell. BA list membership is thus a very important parameter in the efficient set up of a vBTS. If any candidate serving cell is not in the BA List it will be ignored even if it is the strongest cell.
3. If the Location Area Code (LAC) is different between the current serving cell and a candidate serving cell, then the Cell Reselect Hysteresis (CRH) value is also used. CRH is added by the mobile device to the C2 value so that the total of C2 plus CRH (of the current serving cell) must be exceeded by the candidate BTS (or vBTS) C2 before it can be accepted as the new serving cell. Note: CRH is always a factor in setting up a vBTS because the LAC of the CoSCA must be different from the LAC of the MNO BTS in order to extract IMSI/IMEI identity during the process of a location update. This is the technique used by all such GSM vBTS systems. This means the value of the serving cell CRH cannot be ignored. This can be expressed as: $(C2)_{CandidateServingCell} > (C2 + CRH)_{CurrentServingCell}$.

The collected parameters and information must be analyzed to determine the appropriate values that will be used to configure the inner and outer vBTSs, which form part of our system. Note that this process is usually done when commissioning a new controlled area or periodically thereafter when significant changes in the surrounding RF environments are observed.

As shown in Fig. 2, the C2 (i.e. with the CRO) and cell reselection hysteresis (CRH) value can be configured in the inner and outer vBTSs to set the boundaries for attracting or releasing an MS to/from our system. As stated above, to attract an MS to the inner or outer vBTS in our system, we must configure the C2 value of the vBTS to be higher (say 12 dB) than the sum of the C2 and CRH values of the serving BTS. For the MS to be released from our system on exit from the CoSCA, it must switch from the inner vBTS to an MNO BTS with a higher C2 value than the sum of the C2 and CRH values of the inner vBTS which occurs naturally as the MS leaves the CoSCA area.

The two (inner and outer) vBTSs are connected to the BSC via an Ethernet connection. The BSC controls the inner and outer vBTSs using TCP/IP protocol over the Ethernet connection. Note that all the roles and decision making is done in the CMS and not in the vBTS or BSC. When an MS approaches a controlled area, it is attracted by the outer vBTS first by Idle Mode Reselection and interrogated for its IMEI and IMSI identities, which are passed to the CMS through the BSC. The MS is held by the outer vBTS pending further action and the logic of the CMS as follows. As the MS approaches the gate to the controlled area and enters the coverage area of the inner vBTS, it is attracted to the inner vBTS by Idle Mode Reselection and interrogated for its IMEI and IMSI numbers, which are also passed to the CMS. If the MS does not enter the controlled area but moves away it is released back to the MNO by Idle Mode Reselection. If the MS is in the CMS Whitelist it is immediately and always released back to the MNO.

Fig. 2 C2 and CRH value effect on attracting/releasing an MS to/from the system

At the CMS, the following parameters are checked: first, whether the MS was attracted by the outer or inner vBTS and second, whether the MS is included in the allowable list of devices in that controlled area (white list). Based on these parameters, the system takes the following actions:

1. If an MS that is currently uncontrolled is detected first by the outer and then the inner vBTS in that order, and is not included in the whitelist (case 1 in Table 1) the system will control that MS.
2. If an MS that is currently uncontrolled is detected first by the outer and then the inner vBTS in that order and is included in the whitelist (case 2 in Table 1) the system will NOT control that MS.

Table 1 CMS action

Case	First rule		Second rule	State
	Detected by outer vBTS	Detected by inner vBTS	MS in whitelist	
1	Yes	Yes	No	Controlled
2	Yes	Yes	Yes	Uncontrolled
3	Yes	No	No	Uncontrolled
4	Yes	No	Yes	Uncontrolled
5	No	Yes	No	Controlled/ uncontrolled
6	No	Yes	Yes	Uncontrolled

3. If an MS that is currently uncontrolled is detected by the outer vBTS only and is included in the whitelist (case 3 and 4 in Table 1) the system will NOT control that MS.
4. If an MS that is currently uncontrolled is detected by the inner vBTS only and is included in the whitelist (case 6 in Table 1) the system will NOT control that MS.
5. If an MS that is currently controlled (case 1 in Table 1) is detected by the outer vBTS, the system will release (uncontrol) that MS after a waiting period.

Note that in case 5 in Table 1 where an MS is detected by the inner vBTS only and not first by the outer vBTS, implies that the MS has entered the controlled area either via an uncontrolled entrance (e.g. another entrance that is not covered by the outer antenna) or in an OFF state and was subsequently turned ON inside the controlled area. To mitigate this risk, the MS can be controlled or uncontrolled based on the decision of the keeper of the controlled area. If the inner antenna coverage is well controlled and does not spill over the boundaries of the controlled area, the MS in this case will be controlled. Alternatively, if the inner antenna is found to spill over outside the controlled area, it is better to keep the MS uncontrolled to avoid controlling a MS that is located next to the outer boundary of the controlled area (MS III) in Fig. 2.

4 System Prototype and Empirical Results

To validate the system, an area to be controlled was chosen in which to carry out the experiment. The experiment included setting up all the necessary hardware and software, an RF survey of the area to be controlled, programming the vBTS units with the appropriate parameters to mimic the valid BTS in the BALIST of the serving cell and then validating the control scenarios stated in Table 1. The area had the following specifications: 30 meters wide by 15 meters long open office space. The average number of mobile devices in the area at any time was about 25 devices consisting of a variety of MS brands ranging from legacy phones (e.g., Nokia N95) to advanced smartphones (e.g., iPhone, Blackberry, and Samsung Galaxy).

In addition to the collection of configurable vBTSs, commercial off-the-shelf (COTS) antennas, a BSC, CMS, and SAGEM OT460 GSM test phone were also used in the experiment. We started by identifying the CoSCA, and then we conducted field measurements in the controlled area using the SAGEM OT460 test phone to collect the BSIC, BA list, cell ID, LAC, MNC, MCC, CRH, CRO and Rx level values transmitted by nearby BTSs. The collected data was analyzed to select appropriate values for use in configuring the vBTSs.

Table 2 Typical vBTS configuration parameters

Configuration parameter	Potential values	Description	Parameter type
BA_LIST	701,708,712,715	Represents the neighboring channels	Optional
BAND	1 or 2	1: EGSM 900 band, 2: DCS 1800 band	Mandatory
LAC	125	Location Area Code	Mandatory
MNC	112	Mobile Network Code	Mandatory
MCC	655	Mobile Country Code	Mandatory
SET_ARFCN	701	Transmission channel	Mandatory
LOC_REJ_CAUSE	13	Roaming not allowed in this LAC (for Whitelisted MS)	Mandatory
CELL_RESELECT_OFFSET	10	CRO value	Optional
MAX_TXPOWER	13	Transmission power	Mandatory
CELL_ID	34178	Transmission channel cell ID	Mandatory
NCC	255	Network color code	Optional
BSIC	41	Base Station Identity Code	Mandatory

Table 2 highlights the vBTS parameters that must be changed (Mandatory) and may be changed (Optional) based on the situation.

The choice of vBTS ARFCN (in this case 701 which is DCS 1800 MHz GSM) is made by selecting an ARFCN that is present (if possible) in all the BA Lists of the strongest MNO cells so that it can be a candidate serving cell, but which is also one of the weakest to reduce interference with the MNO cell that is using the same ARFCN (frequency).

The BA List (a list of candidate serving cell ARFCNs) that will be broadcast by the vBTS has the function of assisting mobile BTS selection when the mobile is in Idle Mode (by Idle Mode Reselection) between the Inner/Outer vBTS ARFCN and can assist in making it easier or more difficult for the mobile to move back to the PLMN (MNO). If the BA List has only the ARFCN of the two Inner/Outer vBTS (e.g. 701 in Table 2) then it will tend to keep blacklisted mobiles attached. If it also includes neighboring MNO BTS ARFCNs then it will be easy for the blacklisted mobile to move back to the PLMN network.

The LOC_REJ_CAUSE parameter is the parameter to be used to reject the Location Update Request for the whitelisted mobiles. This Location Update Request is made by the mobile phone on entering the CoSCA which has a different LAC from the MNO LAC. The LU Reject Cause value 13 is called “No roaming allowed on this LAC”—once a mobile receives this reject Cause it will not try to camp on to the same LAC (vBTS) again. If the mobile is to be blacklisted the Location Update Request is accepted and the mobile camps on to the vBTS.

Other parameters that depend on the RF environment include, for example, the ARFCN, MCC, MNC, BSIC and Cell ID values taken from the operator Public Land Mobile Network (PLMN) information. These values are located in the BCCH ‘System Information Type 3’ message illustrated in Fig. 3 and found in the SAGEM test phone log.

Note that the LAC value found in the ‘System Information Type 3’ message of the SAGEM test mobile is represented in hexadecimal and must be converted into decimal before being used to configure this vBTS. As stated previously the LAC value used in the vBTS must be

Fig. 3 System Information Type 3

IDLE	BCCH	BSIC	Rx	Cell ID	LAC	PLMN	C1	C2	C31	C32	RM	Tx	Hyst	Off.	Prnly
Serv.	785	4.7	-78	17279	355	420 01	25	29	xxx	xxx	-102	0	8	4	20
N #1	777	5.1	-93	17278	355	420 01	9	13	xxx	xxx	-102	0	8	4	20
N #2	767	3.3	-104	xxx	351	420 01	xxx	xxx	xxx	xxx	-102	0	8	4	20
N #3	775	5.3	-103	12287	399	420 01	-1	3	xxx	xxx	-102	0	8	4	20
N #4	778	6.6	-103	18498	355	420 01	-1	3	xxx	xxx	-102	0	8	4	20
N #5	771	5.0	-106	xxx	xxx	xxx	xxx	xxx	xxx	xxx	xxx	xxx	xxx	xxx	xxx
N #6	101	xxx	xxx	xxx	xxx	xxx	xxx	xxx	xxx	xxx	xxx	xxx	xxx	xxx	xxx

Fig. 4 Serving cell and neighboring ARFCN

different from the LAC values used by the PLMN (here 0x18F or 399 decimal), otherwise the vBTS will not attract any mobile stations and capture the IMSI/IMEI identities. The MCC/MNC (Mobile Country Code and Mobile Network Code) is the same as the PLMN code found at the first 5 digits of any IMSI (SIM card) identity.

Next, the BA list and Absolute Radio Frequency Channel Number (ARFCN) parameters for the vBTS are chosen by forcing the SAGEM test phone into the desired GSM band to see the available neighbor ARFCNs and their signal strength rankings and then forcing the SAGEM onto each of the higher power BTS in turn. Note that this list is actually the list of the 3–4 highest power BTS which are members of the BA List that is periodically broadcast by the serving cell (refer to ARFCN 785 in Fig. 4 for an example).

As stated above, to avoid conflict and overlap between the vBTS and the MNO serving cell, it is also important to avoid emulating the strongest/serving cell in the desired band for example, serving cell 785 shown in Fig. 4, which has an Rx received power of -78 dB, if possible, unless the serving cell Rx power is between -70 and -90 dB and there are no neighboring channels.

The figure also lists five neighboring ARFCN channels. Only channels with complete data including BSIC, Rx, Cell ID, LAC, PLMN, C1, and C2 information should be used to emulate a legitimate BTS so that cell parameters can be optimally cloned. Channel numbers 777, 775, and 778 are the only channels with complete sets of data and are not serving cells with similar C2 values; therefore they all have a more or less equal chance of selection for the vBTS clone. In the current example, we could choose channel 775, we will use the following values to configure the vBTS:

- Cell ID = 12287 we can use this value from the PLMN
- LAC = 399 for the MNO but we need to be different so we would choose say 123 for the vBTS
- BSIC = 5.3, which needs to be converted into a decimal value, that is, $5 \times 8 + 3 = 43$
- The CRO is 4 (see “Off”) but we can choose a value as needed probably about 10 dB to boost the apparent power
- The CRH is 8 (see “Hyst”) but we can choose a value as needed probably about 8 dB to keep the MS attached

The values for the vBTS on the inner side of the CoSCA were set up in a similar way, on a different ARFCN and LAC. The next step in the experiment involved programming the vBTS with the values given above.

We used a number of handsets in different test scenarios. In the following we describe the field results obtained from executing the cases described in Table 1. In the experiment, we used 4 MSs: MS1 and MS2 (Nokia 1200 handsets with IMSI1 and IMSI2) were included in the whitelist, whereas MS3 and MS4 (Nokia N95 handsets with IMSI3 and IMSI4) were not included in the whitelist and thus subject to be controlled by our system.

All four MSs were detected first by the outer antenna on their way into the controlled area. Once all four MSs were inside the controlled area, they were detected by the inner antenna, which triggered the BSC to pass their information to the CMS to execute the detection rules as described in Table 1. Because MS1 and MS2 were included in the whitelist and were allowed to operate in the designated controlled area, the CMS instructed the BSC to issue Location Update rejection code 13 to MS1 and MS2, disengaging them from our system and allowing them to reconnect with the MNO serving cell. Because MS3 and MS4 were not included in the whitelist and were not allowed to operate in the designated controlled area, the CMS did not instruct the BSC to issue a Location Update rejection code 13 to MS3 and MS4 thus keeping them connected to our system and disallowing them from connecting to any MNO serving cell while they were within the controlled area.

If either of the controlled MSs (3 or 4) were to leave the controlled area, the outer antenna would be triggered on its way out. Being detected by the outer antenna after being in a controlled state, result in the CMS instructing the BSC to issue Location Update rejection code 13 to that MS, disconnecting it from our system and allowing it to reconnect to the MNO serving cell.

All cases described in Table 1 were tested successfully and results were as expected. The limitations observed in the current system configuration were as previously stated when a MS was brought into the controlled area through another entrance (another doorway, window, etc.) and did not go through the outer and inner antennas. Another limitation was observed when a MS was brought into the controlled area in an OFF state and was turned ON inside the controlled area. In the case when a MS enters a controlled area while in the dedicated mode (middle of a call), our system could not attract the MS by Idle Mode Reselection, and therefore could not control it.

In some cases, certain MS brands were not automatically detected by the system which required some updates to the vBTS scripts to include it. This is a once of exercise that might be needed when commissioning the system or as part of the system maintenance to make sure newly released MSs are detectable by the system. A notable example is the use of 3G mobiles which have a preference to remain on UMTS served by the MNO rather than moving to GSM supported by these vBTS. In addition, it is required to have sufficient vBTS units to cover all the bands and PLMNs if it is required to control all mobiles attached to any PLMN at the same time.

4.1 Performance Evaluation

The effectiveness of the proposed system can be evaluated based on the following parameters:

- The percentage of MSs that were successfully controlled out of all MSs that entered the CoSCA.
- The percentage of MSs that are located nearby the CoSCA—but not within its boundaries—that are unintentionally controlled.
- The average time needed to control a MS after entering a CoSCA.

Table 3 Reliability test results

Period (min)	Number of mobile test cases attached to vBTS	% of all mobile test cases
0–3	98	76.6
4–5	14	10.9
6–10	10	7.8
Over 10	5	3.9
Within 15	127	99.2

To measure such parameters, a test was conducted using vBTSs that support GSM for two MNOs in the controlled area. A total of 128 GSM mobile test cases were done. Out of that number, 127 were successfully attached to the vBTSs and delivered their IMSI/IMEI numbers within 15 min as shown in Table 3.

The minimum time to attract and control a MS was 14 s, while the maximum was 14 min and 22 s and the average was 1 min and 25 s.

As for the percentage of MSs that are located nearby the CoSCA—but not within its boundaries—that are unintentionally controlled, test results showed that the level of mobile attraction was down to 20 % or less at 6 meters from the controlled area walls. This equates to occasional blocking of less than 20 % of mobiles in that area after 3 min.

5 Conclusion

A novel system for controlling mobile communication services in areas where complete silence is either expected or mandated, including schools, universities, places of worship, hospitals, and jails was presented. The method includes identifying, through a base station controller and a sequence of detection steps when a mobile device is within the area to be controlled. The method has been prototyped and demonstrated using COTS and custom designed hardware and software subsystems. Survey results have been offered to demonstrate effective MS control while limiting unwanted RF “spillage” and MS control from a controlled area.

6 Further Work

6.1 Support for UMTS

The system described above uses several GSM vBTS units to attract GSM mobiles. Clearly, many mobiles are capable of 3G support and if attached to the 3G (UMTS) network will not normally be attracted to the described system—especially if the user has disallowed GSM network roaming. Work is in progress to test a 3G capability to supplement the 2G capability.

6.2 Using Leaky Feeders in the Controlled Area

A problem often seen in tests with directional antennae is unpredictable spillage of RF and reflections from the controlled area inner antenna so that the logic determining if a mobile is inside or outside the controlled area may sometimes be confused. Further work is indicated by the use of a radiating antenna (sometimes called a leaky feeder) inside the controlled area. The leaky feeder relies more on the Near Field and its signal falloff with distance is quicker allowing more localized control in and near the controlled area [12].

6.3 Possible Application in Convoy Protection

The concept of controlling a specific area can be extended to include non-stationary or moving class of service controlled areas (Mobile CoSCAs). A mobile CoSCA can be useful to control mobile communication within a bubble of coverage in a moving car for example. This system can be useful in VIP convoys where only the VIP and guards phones can be allowed to communicate and included in the whitelist, while all other unknown devices within the coverage area of the mobile vBTS will be controlled and therefore will not be allowed to connect to any serving base station. This will eliminate their usefulness in triggering any attacks on the moving vehicle [13]. Several challenges need to be researched especially in relation to a critical application such as a moving convoy where the goal requires close to 100 % success.

Acknowledgments This work was supported by King Abdulaziz City for Science and Technology under Project: Design and Development of Mobile Station Class of Service System, National Science, Technology and Innovation plan (NSTIP) Grant Number 31-459.

Open Access This article is distributed under the terms of the Creative Commons Attribution License which permits any use, distribution, and reproduction in any medium, provided the original author(s) and the source are credited.

References

1. Pinyapong, S., Shoji, H., & Kato, T. (2007). Mobile information service adapted to social, temporal and dynamic situational requirements of individuals. In: *Proceedings of 2007 IEEE Asia-Pacific services computing conference*, Dec. 2007, pp. 517–520.
2. Acampora, A., & Naghshineh, M. (1994). Control and quality-of-service provisioning in high-speed microcellular networks. *IEEE Personal Communications*, 1(2), 36–43.
3. Behairy, H., Alhumaidi, S., Alrobian, W., Alghammas, A., Almansour, I., Dabil, A., et al. (2013). *Controlled mobile communication in a socially sensitive environment*. USPTO 8346241, Jan. 1, 2013.
4. Behairy, H., Alhumaidi, S., Alrobian, W., Alghammas, A., Almansour, I., Dabil, A., et al. (2013). *Controlled mobile communication as a service*. USPTO 8428574, April, 23, 2013.
5. Efsthathiou, E. (2002). *The mobile-phone silencers controversy*. Athens: Athens University of Economics and Business, Department of Computer Science, Mobile Multimedia Library.
6. Antonini, G., Orlandi, A., & D'elia, S. (2003). Shielding effects of reinforced concrete structures to electromagnetic fields due to GSM and UMTS systems. *IEEE Transactions Magnetics*, 39(3), 1582–1585.
7. Mishra, N. (2009). Development of GSM - 900 mobile jammer: An approach to overcome existing limitations of jammers. In *Proceedings of 5th IEEE conference on wireless communication and sensor networks (WCSN)*, Dec. 2009, pp. 1–4.
8. Abu-Amara, M., & Mahmoud, M. (2008). *Method of non-intrusive control of mobile device*. USPTO Pub. No.: US 2008/0113657 A1, May 2008.
9. Hong, J., & Bilstad, A. (2010). *Methods for ring tone suppression informing and for informing a cellular telephone with configuration data*. USPTO 7668557, Feb. 23, 2010.
10. Hsu, J. & Regan, R. D. (2013). *Controlling device functions of a mobile terminal in a restricted area*. USPTO US20130225086 A1, Aug. 29 2013.
11. 3rd Generation Partnership Project 3GPP TS 45.008, Radio subsystem link control, V11.2.0 (2012–08), (Release 11) pp. 20–21.
12. Behairy, H., Alrobian, W., Alghammas, A., Alsuwayyeh, Y., Alqunaieer, F. (2014). *Controlled mobile communication as a service in a coverage area bounded by radiating cables*. USPTO Application 20130217376, allowed Feb. 12, 2014.
13. Behairy, H., Alhumaidi, S., Alrobian, W., Alghammas, A., Almansour, I., Dabil, A., et al. (2013). *Selective control of a wireless service associated with a mobile device*. USPTO 8417237, Apr. 9, 2013.

Hatim M. Behairy received his M.Sc. in Electrical Engineering and Ph.D. in Information Technology from George Mason University, Virginia, USA in 1997 and 2002, respectively. He has been with the National Electronics, Communication, and Photonics Center at King Abdulaziz City for Science and Technology, Riyadh, Saudi Arabia since 2003. His research interests are in the design of new error correction coding techniques for next-generation broadband wireless communication systems using turbo-coding principles.

Waleed S. Alrobian received his M.Sc. in computer science from RMIT University, Melbourne, Australia in 2009. He has been with the National Electronics, Communication, and Photonics Center at King Abdulaziz City for Science and Technology, Riyadh, Saudi Arabia since 2005. His research interests are in Cloud computing security and Mobile Web-services security.

Adnan A. Alghammas received his B.Sc. in Electronics and communications engineering from King Saud University, Riyadh, Saudi Arabia in 2009. He has been with the National Electronics, Communication, and Photonics Center at King Abdulaziz City for Science and Technology, Riyadh, Saudi Arabia since 2009. His research interests are in Wi-max Technology.

Brian R. Suter received his B.Sc. in Electrical Engineering from the University of Cape Town, South Africa in 1982. He has been with Tellumat (Pty) Ltd in Cape Town South Africa since 2005 and was involved in many projects over the years in Telecoms and more recently in collaboration with King Abdulaziz City for Science and Technology.