Embedded Subscriber Identity Module with Context Switching

Kaushik Sarker and K. M. Muzahidul Islam(✉)

Department of Software Engineering, Daffodil International University, Dhaka, Bangladesh
kaushik.swe@daffodilvarsity.edu.bd,
muzahidul670@diu.edu.bd

Abstract. Telecommunications technology user wants quality channels including security, customization, personalization and autonomy. These requirements are encouraging customers to use multiple identity modules. Use of multiple modules brings the necessity of caring multiple cellular phones or multiple cellular units in a mobile device. Moreover, the switching between the identity module is physical and less secure with the possibility of an identity module cloning or loss of module in case of theft. Several research works have been found in the area of embedded Subscriber Identity Module (eSIM) and Virtual Subscriber Identity module (VSIM). However, the limitations of both eSIM and VSIM have given the authors of this paper a scope to study and come up with a solution by proposing a new model. In the proposed model authors have considered the benefits of eSIM and VSIM together and reducing the limitations such as switching between the modules, parallel activation of the modules, module cloning etc. At the end of the paper, authors have compared ten such limitations, known as features with the existing models and presented a graphical simulation of the proposed model with the proposed methodology of context switching between embedded subscriber identity modules.

Keywords: eSIM · VSIM · Multiple SIM activation · SIM Context Switching · Subscriber Profile Manager

1 Introduction

Gradually consumers are shifting from the bulky device to tiny device. Moreover, their needs have grown up invariably. On the contrary, mobile companies are trying to connect customers' needs into a small space [7]. In this circumstance, the conventional removable SIM device has occupied a large amount of space and created some limitation as SIM can be removed and cloned without user's permission which has created vulnerability by producing immoral activities.

Each device holds IMEI which is stored unsafely into the device. Moreover, IMEI Tracking Technology is not accessible to the public and many of them do not conserve the IMEI number in a safe place. Besides, IMEI number can be changed or masked.

GSMA introduces Embedded Subscriber Identity Module (eSIM) technology to overwhelm some vulnerabilities of removal SIM and this technology stores the

A. B. Gani et al. (Eds.): ICICCT 2019, CCIS 1025, pp. 84–97, 2019.
https://doi.org/10.1007/978-981-15-1384-8_8

customer identity profiles and installs it to the device through a central server [3]. In contrast, the VSIM concept is the revolution of ensuring user autonomy. However, unsafe IMEI problems are still present. After the introduction the limitation of eSIM and VSIM have been discussed in the literature review. Next, in the research methodology section a conceptual architecture has been proposed. After that, a simulation is provided in the result and discussion section along with the comparison between existing and the proposed model and finally concluded in the next section.

2 Literature Review

Inadequate network coverage led to the interrupting of communication. Besides, different network operators offer special tariffs with different bundles. On the other hand, customers do not want to detach the old number. As a result, consumers are motivated to use multiple Subscriber Identity Modules one for personal and one for official use, etc. [13].

2.1 Architectures with Their Limitations

GSMA eUICC Architecture. Embedded UICC (eUICC) requirements, definitions, roles and procedures are standardized by European Telecommunications Standards Institute in the year 2013 [15]. Besides, GSMA develops a standard specification based on ETSI which covered OTA installations, enablement, disablement and profile deletion process to the eUICC [4].
Proprietary five interfaces (1) Subscription Manager-Data Preparation (SM–DP), (2) Subscription Manager–Secure Routing (SM–SR), (3) Mobile Network Operator (MNO), (4) Certificate Issuer, and (5) eUICC Vendor have been connected to eight technical connection of OTA profile management which helped enough to well-define the eSIM technology [15]. Moreover, it is a rewritable built-in hardware component that allows the SIM profile installation remotely over the air by a Mobile Network Operator (MNO) through a universal server [1] which has three categories namely (1) machine to machine (M2M), (2) Machine to Person (M2P) and (3) Hybrid. Besides, four groups of players are involved, they are (1) eSIM Vendor, (2) Original Equipment Manufacturer (OEM), (3) Mobile Virtual Network Operator, and (4) Independent Profile Manager. In contrast, to serve this technology to the consumer, three network configurations have been maintained namely (1) OEM-Centered, (2) MNO-Centered, and (3) Independent Party. However, Mobile Network Operator (MNO) sells M2P categories eSIM. Although, this technology has been designed to reduce the space and cost of the device including multiple SIM Profiles installation without considering simultaneous activations. Nonetheless, in this technology to change the SIM Profile, it does not require exchange of physical components [3–6]. Besides, eSIM technology reduced integration, testing and handling costs for M2M SIM products which have done a little change and used existing SIM factors including (1) MFF1, MFF2 for embedded, (2) 2FF, 3FF for removable and same hardware component [5].

Limitations of GSMA eUICC Architecture. Performance and security issues including lacking in requirements [9, 11] have been found out through analyzing all documents and thirteen eUICC procedures including Registration, Profile Verification, Ordering, Download and Installation, Enabling, Disabling, etc. [4, 13, 14]. Many of the security issues already solved by author A. Vesselkov [15]. However, some limitations still exist and they are related to problem with multiple SIM activation, sharing of contact from inactive SIM, longer response time, managing profile remotely by subscriber.

2.2 Virtual SIM (VSIM) Architecture with Limitations

Virtual SIM (VSIM) Architecture. Virtual Subscriber Identity Module (VSIM) which is introduced in the year 2012 provides different framework and technique epitomes for holding and exchanging individual information contained inside the memory of portable handset gadgets. A few with versatile handset with the capacity to download individual information to a server after validation and Verification, whereas, a few use alphanumeric passwords for client confirmation and check purposes [12].

Limitations of Virtual SIM (VSIM). VSIM is the first concept where user autonomy has been ensured by providing some legal management power. However, some lack of requirements, performance and security issues still present [12], which are related to issues of SIM cloning, problem with multiple SIM activation and longer response time.

3 Research Methodology

eSIM Context Switching model is a combination of eSIM [3–5] and VSIM [12] model. Although, some modification has been made to reduce cost, space and increases usability. Moreover, this modification also reduced the eSIM and VSIM limitations which are mentioned before. The following four primary features have been considered along with six other features while proposing this model.

1. Multiple SIM activation: Multiple SIM activation is done through artificial switching which activate the SIM according to the user activity by integrating M2M [3] with artificial methodology.
2. Sharing: Closed or offline SIM can share necessary data with the device such as a contact list and others.
3. Reducing response time: If SIM is closed, busy, waiting or already has an established voice channel then it can send feedback without requesting the end device which can reduce time than the traditional system.
4. Preventing sim cloning: This model does not allow IMEI modification through the user rather IMEI is updated continuously.

3.1 Proposed System Architecture

Context Switching Model [10, 12].

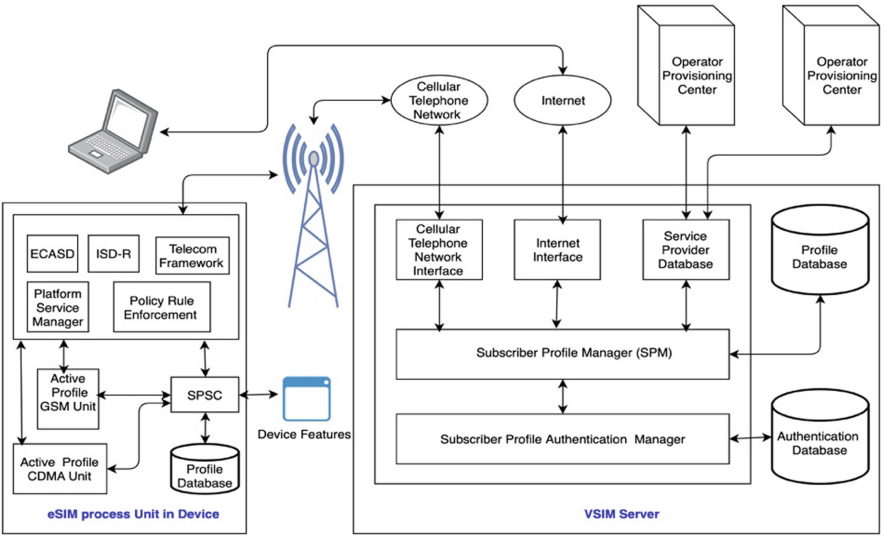

Fig. 1. Context switching model diagram.

Profile Activation/Deletion By network Request.

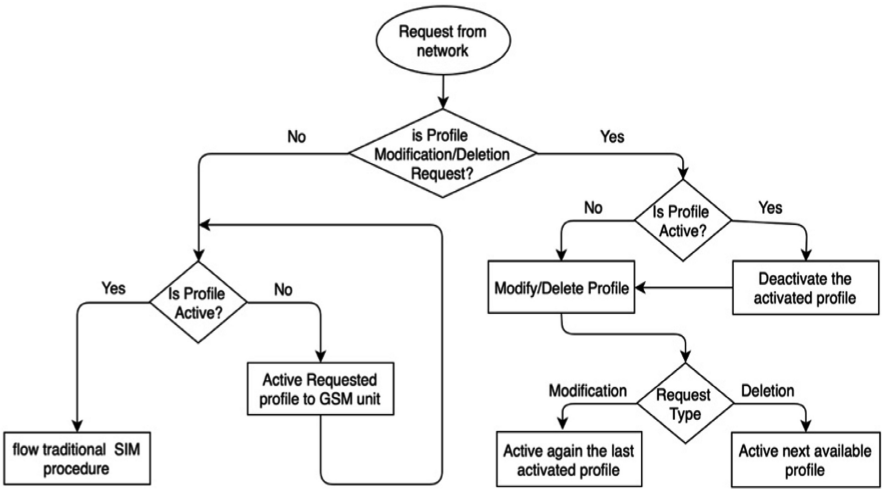

Fig. 2. Profile activation/deletion by network request (in device)

Request routing through Subscriber Profile Manager.

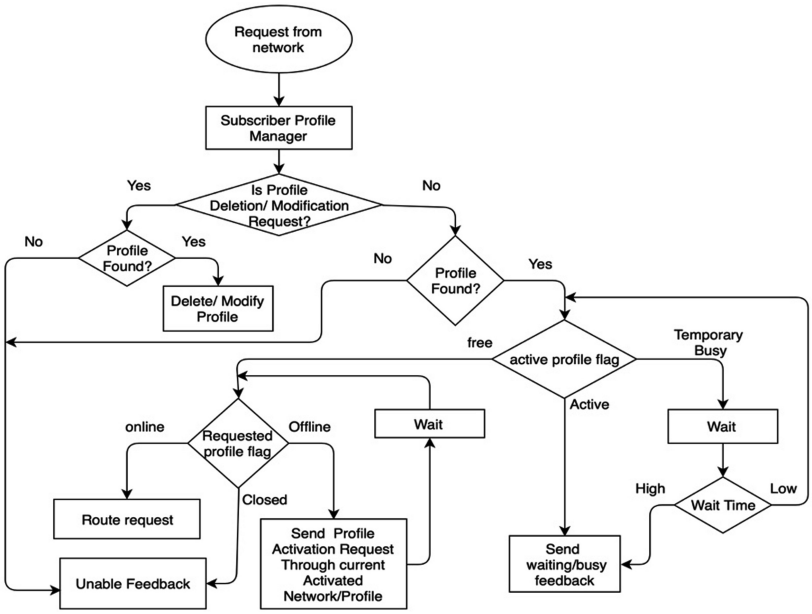

Fig. 3. Request routing through subscriber profile manager (Server)

3.2 Status Flag Details

The flag is a predefined bit which is used for leaving a sign for other programs, communicating M2M or to remember something [2]. In this model, flag has been used to communicate between the Subscriber Profile Switching Center (SPSC) and Subscriber Profile Manager (SPM).

Network. This type of flag can be set on the request header to send data to server and device (Table 1).

Table 1. Network readable flags with actions

No	Flag name	Action	Directions
1		This flag can be set by SPSC or SPM on header of the data packet	Server to Server Device to Server
2	Device	This flag can be set by SPM on header of the data packet	Server to Device

Profile. This type of flag can be set through the device into the server profile database (Table 2).

Table 2. SPSC or SPM readable flags with actions

No	Flag name	Action
1	Active	When any communication channel has to be established between two end device then active profile can be set
2	Online	It does indicate that Profile is active and it has established network
3	Offline	This flag denoted that currently profile not active or has not established network but it can be active by SPM request
4	Closed	It does indicate unable to activate this profile
5	Temporary Busy	If activate profile receive any data or signal for a while then this flag can be set to the profile
6	Busy	This flag denoted that it can handle only message request

3.3 Profile Database

Profile database [12] must be at least four attributes, namely (1) serial no, (2) profile raw data, (3) flag, (4) IMEI. This table's name may have depended on the user's primary key. Profile flag and IMEI must have updated continuously through the device.

3.4 Steps of Context Switching Model

1. ECASD, ISD-R, Telecom Framework, Platform Service Manager, Policy Rule Enforcement will work like eSIM procedure [10] however has to use Subscriber Profile Switching Center (SPSC) as media to communicate with Subscriber Identity Profile, as shown in "Fig. 1".
2. SPSC will activate profile into CDMA activation unit only through own device request. Steps 3 to 14 are only for the GSM network.
3. When procedure 1 handovers the task to SPSC then it will check the request type. Two types of request can be sent by the GSM network, one of them devoted to profile management, As shown in "Fig. 2". Another, will follow procedures of traditional SIM [8].
4. If SPSC gets any other requests except profile related request from SPM then it will follow the procedure of the eSIM, as shown in "Fig. 2".
5. SPSC must have to send all individual Subscriber Profiles flag (online, offline, etc.) and all information of the device (IMEI, etc.) to the SPM continuously.
6. If there is any data header that contains the SERVER or DEVICE flag then MNO must have to be proceed.
7. Cellular Telephone Network Interface, Internet Interface, Service Provider Database and Subscriber Profile Authentication Manager will follow the VSIM procedure [12]. But it has to use SPM as a media to handle SERVER flagged request or any database related request.
8. Traditional network procedure will be followed when the SERVER or DEVICE flag is missing [8].
9. In the end device, the eSIM procedure will be followed to SIM installation and deletion [10] but it has to be handed over to the SPSC before the final stage of the

procedure. In the server part, the VSIM procedure will be followed to SIM deletion and installation [12] but it has to hand over to the SPM before the final stage.

10. Subscriber Profile Manager (SPM) can get two types of network requests, one of them is Profile related and another is routing related. Both requests first check profile existence from Profile Database, if the profile does not exist then sends acknowledgment which is shown in "Fig. 3". On the other hand, if the profile exists then it follows step 11 or 12.
11. If SPM gets profile deletion or modification request through remote source then it routes that request to SPSC and waits for feedback before action. When it gets feedback from end device then it triggers the action.
12. If SPM gets routing request then it considers profile status, there are three types of profile status available. Profile flags with actions (Table 3).

Table 3. Actions for profile flag of active profile

Profile flag name	Condition check	Action
Temporary busy	Wait time high	Wait few moments and check again its profile
	Wait time low	Send busy feedback
Active	Null	Send waiting/Busy feedback
Free	Null	Flow procedure "12"

13. To route the request, it checks three types of flag for the requested profile to take further actions. Profile flag with actions (Table 4).

Table 4. Actions of Profile Flag of Requested Profile

Profile flag name	Action
Online	Route the current request
Offline	First send profile activation request to the SPSC and wait and check again.
Closed	Send unable feedback

14. To establish a channel between two devices, communicating with the server is required.

4 Result and Discussion

Proposed eSIM Context Switching model through merging two systems [3, 12] with the mentioned steps is compared in the following table with eSIM and VSIM. From the table it is observed that the proposed model solves all mentioned issues related to previously mentioned features (Table 5).

Table 5. Features comparison with proposed model

No	Features	eSIM	VSIM	Proposed model
01	Multi profile active	No [3–5, 15]	No [12]	Yes
02	Offline profile can share contacts	No [4]	No [12]	Yes
03	Profile backup from device	Yes [4]	Yes [12]	No
04	Unable or waiting feedback	From Device [4]	From Device [12]	From SPM
05	Unable or waiting feedback processing time	Long [4]	Long [12]	Short
06	User Autonomy	No [4]	Yes [12]	Yes
07	Device owner authentication Required To add profile	Not Specified	Not Specified	Yes
08	Profile owner authentication required to add profile	Yes [4]	Yes [12]	Yes
09	Master password for modification	Not Specified	Yes [12]	Yes
10	CDMA and GSM Active at a time	No [4]	No [12]	Yes

4.1 Simulation of the Proposed Model

Since this a conceptual model, therefore has been proved by developing a virtual simulator where only context switching part has been considered. To test this model in the simulator, three Cellular Network Towers [16], two Dialer Devices [17] and one receiver device [17] have been used (Fig. 4).

Fig. 4. Simulator color specifications.

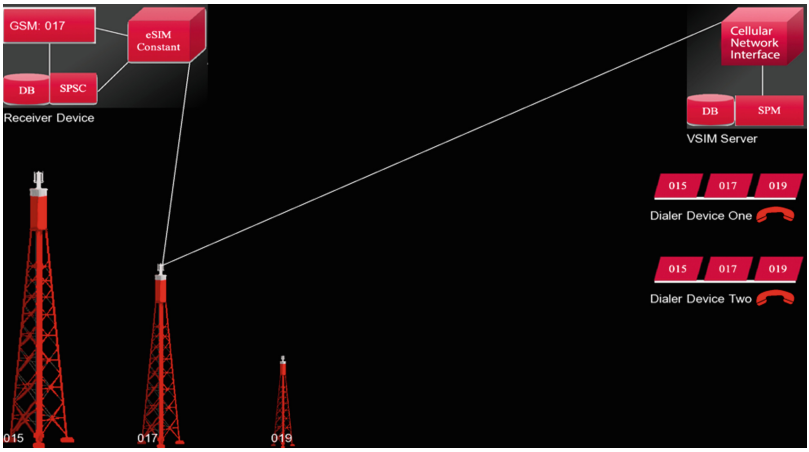

Fig. 5. Simulator initial state.

In "Fig. 5", GSM activation unit, SPSC and eSIM constant have established a regular connection within the receiver device. A regular connection is also established between Cellular Telephone Network Interface and SPM in VSIM server. eSIM constant of Receiver Device has established a regular connection with Cellular Telephone Network Interface of VSIM server through GSM network tower 017.

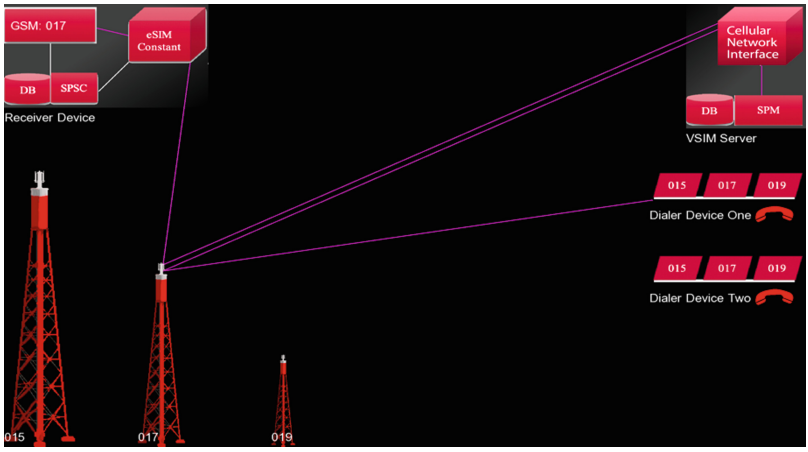

Fig. 6. Dialer one requests through same connection.

In "Fig. 6", Dialer Device One has established a channel with receiver device SIM 017 by following 1 to 4 steps.

1. The request was sent by Dialer Device One to GSM network tower 017.
2. GSM network 017 had to route that request to the Cellular Telephone Network Interface.
3. Cellular Telephone Network Interface had to handover the request to the SPM.
4. SPM had to analyze flags of the requested SIM and had gotten ONLINE flag [Fig. 5]. Therefore, SPM directly has routed the request to the Receiver Device to establish a voice channel.

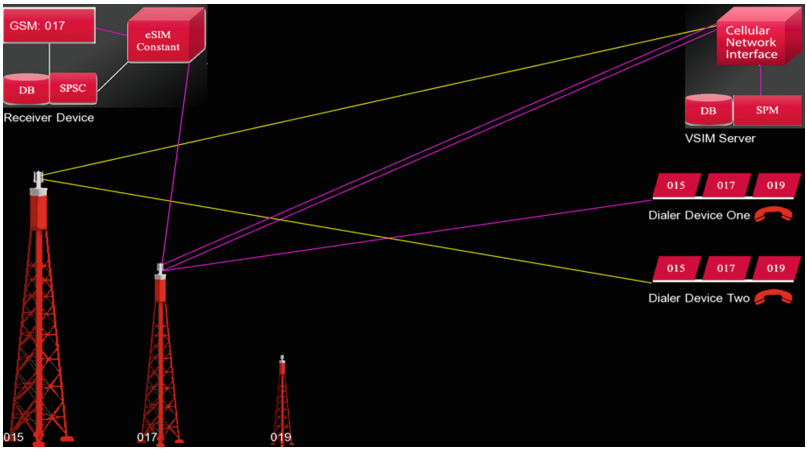

Fig. 7. Dialer two requests for another network.

In "Fig. 7", Dialer Device Two wanted to establish a channel with Receiver Device SIM 015 while having an established channel between Dialer One and Receiver Device SIM 017.

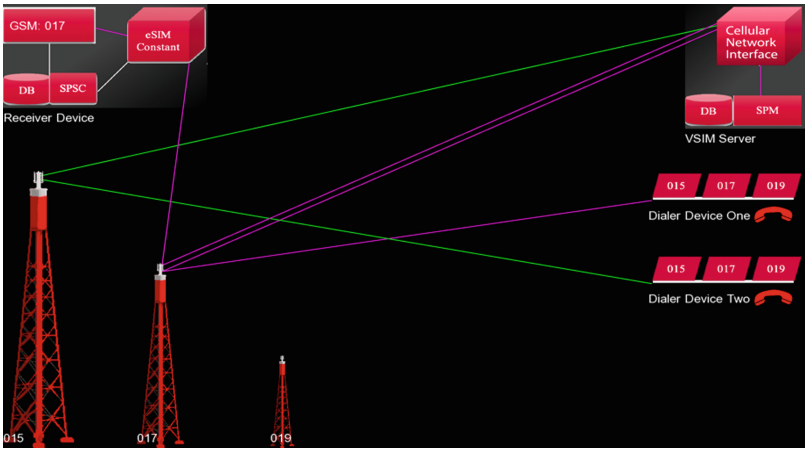

Fig. 8. Server sends activation feedback.

Since Dialer Device One has already an established channel (Active flag), therefore SPM has responded a BUSY flag to the dialer device which is shown in "Fig. 8".

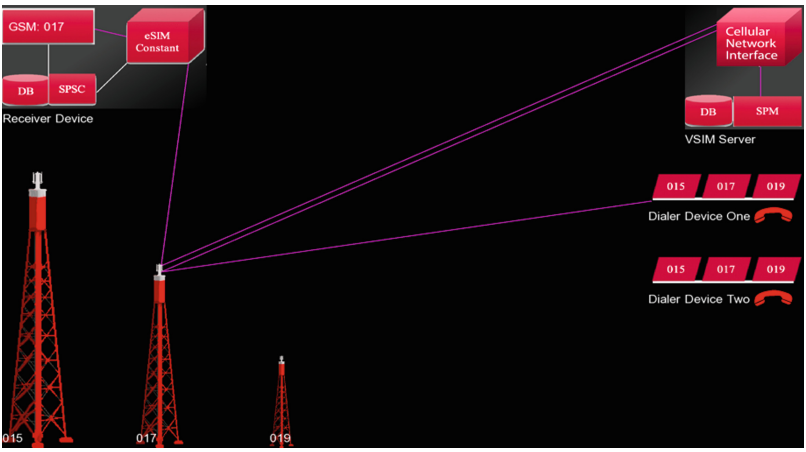

Fig. 9. Request of dialer two rejected.

In "Fig. 9", Dialer Device Two has rejected the request automatically by getting BUSY response from SPM. In "Fig. 10", Dialer Device One has freed the established voice channel.

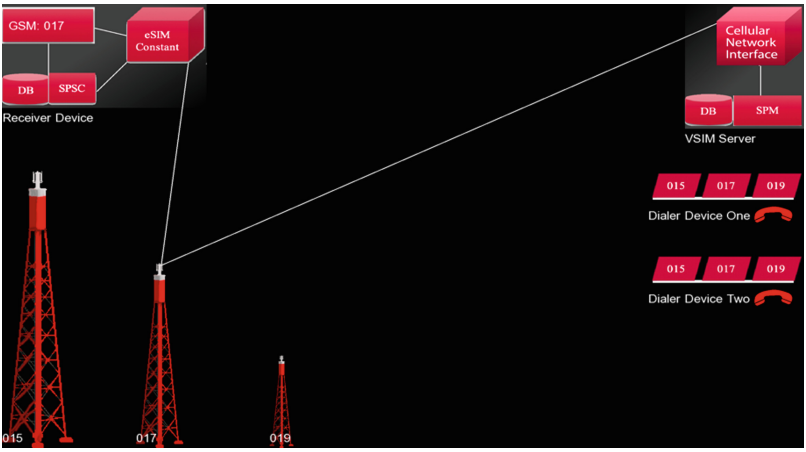

Fig. 10. Dialer one has freed the channel again.

In "Fig. 11", Dialer Device Two wants to establish a channel with Receiver Device SIM 015 but Receiver Device has an active different SIM with the ONLINE flag. Therefore, to establish this channel steps from 1 to 6 have to be followed.

1. Dialer Device Two has sent a request to the Cellular Telephone Network Interface of VSIM server through GSM network tower 015.
2. Cellular Telephone Network Interface has handovered this request to the SPM.
3. SPM has analyzed flags of the requested SIM and has realized an OFFLINE flag. Besides, it also got a different ONLINE flag SIM which is located in same Receiver Device that is wanted by Dialer Device Two. Therefore, SPM has sent SIM Switching request to SPSC through Cellular Telephone Network Interface, GSM network 017 and eSIM constant. Moreover, SPM rechecks again after waiting for a while.

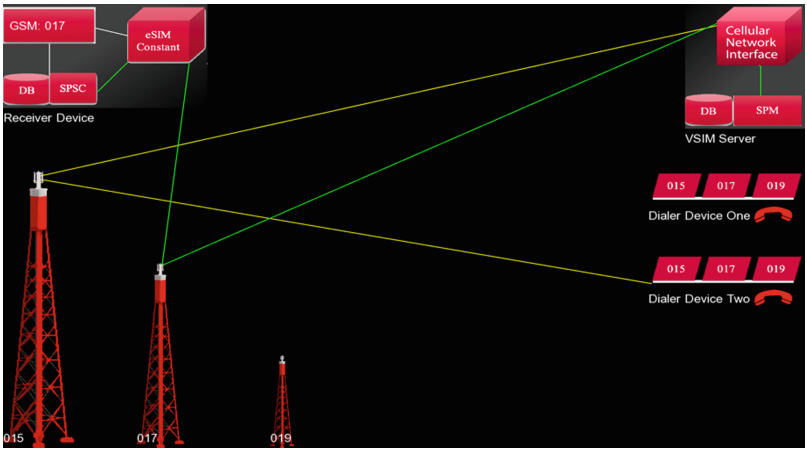

Fig. 11. Dialer two requests again and server sends request to SPSC.

4. eSIM constant has checked SIM flag again. After checking, if ACTIVE flag is not found then it does the route to the SPSC.

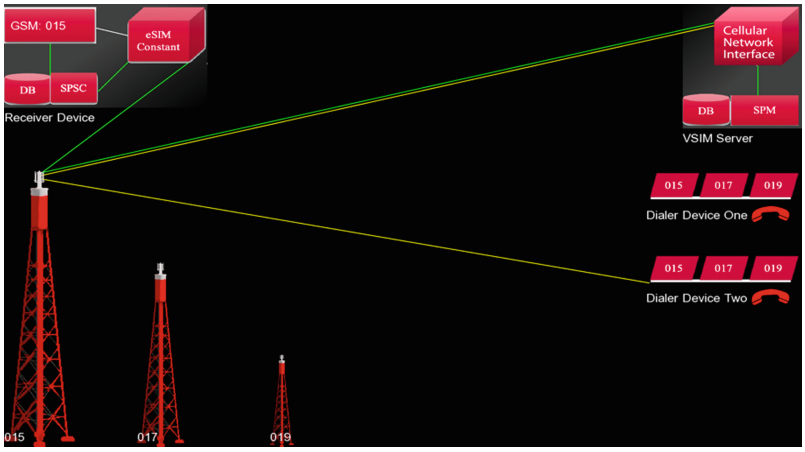

Fig. 12. SPSC has activated requested profile to the GSM Unit.

5. In "Fig. 12", SPSC has activated the requested SIM after removing the activated SIM from GSM SIM activation unit.
6. In "Fig. 13", finally, a voice channel has been established between Receiver Device and Dialer Device Two.

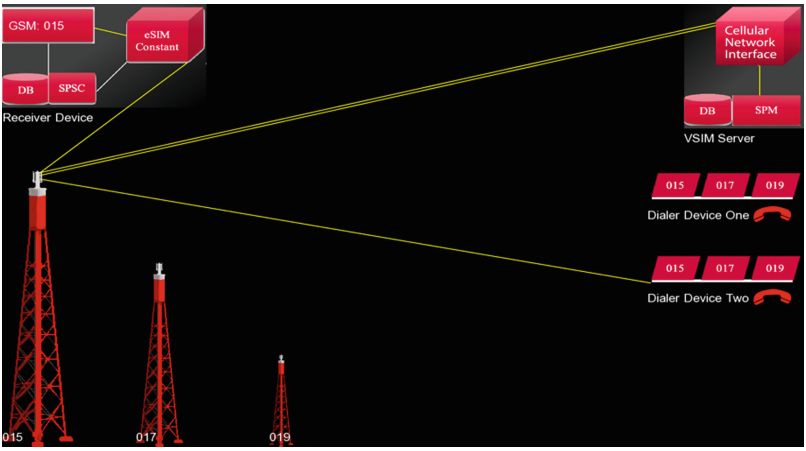

Fig. 13. After profile switching, channel has been established.

5 Conclusion

The main focus of the study was to find out a technique for proper switching between the embedded subscriber identity modules by eliminating the limitations of the existing eSIM and VSIM techniques. By providing the required modification in the existing model and combining the two existing techniques with required modification by introducing the proper methodology of working, the authors have been able to show that their proposed model can handle parallel activation of the modules, reduce the expenses of physical switching, increase the security by eliminating cloning, reduce device theft etc. However, the system did not consider the roaming capability of the SIM during this switching. Moreover, the proposed model is a conceptual one, which in future may be researched and implemented in a real-life device and those may fall under the scope of the future research.

References

1. Bender, H., Lehmann, G.: Evolution of SIM provisioning towards a flexible MCIM provisioning in M2M vertical industries. In: 2012 16th International Conference on Intelligence in Next Generation Networks. IEEE (2012)
2. What is flag? - Definition from WhatIs.com. https://whatis.techtarget.com/definition/flag
3. Gerpott, T.J., May, S.: Embedded subscriber identity module eSIM. Bus. Inf. Syst. Eng. **59**, 293–296 (2017)

4. GSMA, Embedded SIM Remote Provisioning Architecture. https://www.gsma.com/iot/wp-content/uploads/2014/01/1.-GSMA-Embedded-SIM-Remote-Provisioning-Architecture-Version-1.1.pdf
5. GSMA, GSMA Embedded SIM Specification Remote SIM Provisioning for M2M. https://www.gsma.com/iot/wp-content/uploads/2014/10/Embedded-SIM-Toolkit-Oct-14-updated1.pdf
6. GSMA, Leading M2M alliance back the GSMA embedded SIM specification to accelerate the internet of things. https://www.gsma.com/newsroom/press-release/leading-m2m-alliances-back-the-gsma-embedded-sim/
7. Mobile network operator on-demand subscription management study. https://www.ey.com/Publication/vwLUAssets/EY-mobile-network-operator-on-demand-subscription-management/$FILE/EY-mobile-network-operator-on-demand-subscription-management.pdf
8. Mouly, M., Pautet, M.: The GSM system for mobile communications. In: Cell&Sys, Palaiseau, France (1992)
9. Park, J., Baek, K., Kang, C.: Secure profile provisioning architecture for embedded UICC. In: 2013 International Conference on Availability, Reliability and Security. IEEE (2013)
10. GSMA, Remote Provisioning Architecture for Embedded UICC Technical Specification. https://www.gsma.com/newsroom/wp-content/uploads/SGP.02_v3.2_updated.pdf
11. Richarme, M.: The virtual SIM - a feasibility study. Technical University of Denmark, Department of Applied Mathematics and Computer Science, Lyngby, Denmark (2008)
12. Shi, G., Tangirala, V., Durand, J., Dudani, A.: Virtual SIM card for mobile handsets. USA Patent US11963918 (2007)
13. Sutherland, E.: Counting mobile phones, sim cards & customers. SSRN, 10 (2009)
14. Vahidian, E.: Evolution of the SIM to eSIM. NTNU Open (2013)
15. Vesselkov, A., Hammainen, H., Ikalainen, P.: Value networks of embedded SIM-based remote subscription management. In: 2015 Conference of Telecommunication, Media and Internet Techno-Economics (CTTE). IEEE (2015)
16. Erran, L., Morley, Z., Rexford, J.: CellSDN: software-defined cellular networks. In: ACM SIGCOMM, Hong Kong, China (2013)
17. Andrus, J., Dall, C., Hof, A.V., Laadan, O., Nieh, J.: Cells: a virtual mobile smartphone architecture. In: Proceedings of the 23rd SOSP (2011)