Incrementing Bit Fields of Subscriber Identity Module (SIM)

Debabrata Sarddar, Utpal Ghosh, Rajat Pandit

Abstract: ***The overall markets for SIM cards is massive and comparatively Stable. In fact, the amount of SIM cards shipped globally is forecast to extend a huge range and still increasing at once. So, increasing the bit field of MSIN(Mobile Subscriber Identification Number) is additionally an helpful choice to choose. however in present bit size of nine or ten (depends on the country) the MSIN have over trillion mixtures of obtainable numbers. In our proposed work we have a tendency to makes a group of home MNCs that are connects in usual, and Keeps record of attributes like 'Signal Strength', 'Internet Speed', 'Call drop. After that, Orders or sorts the set of MNCs as per any alternative of those attributes, then selects the most effective result for home MNCs each time and Updates the database contiguously.As the population is increasing of the globe and additionally there is no any regulation or an individual is not restricted to use just one SIM card so, it would be a secure possibility for future use.***

Keywords: Subscriber Identity Module(SIM), International Mobile Subscriber Identity(IMSI), ICCID, Bit fields of SIM card, Personal Unblocking Code(PUC), Encryption- decryption rule.

I. INTRODUCTION

An integrated circuit for the TracFone Wireless SIM has no unique carriers and scarcely is marked as a« SIM CARD» that safely retains the International Mobile Subscriber identity variety (IMSI) and its related keys that are used to determining and certifying mobile phone subscribers. Contact details on multiple sim cards can be stored together. SIM cards are used continuously on GSM telephones, and only new LTE-capable telephones for CDMA telephones. SIM cards also can be utilized in satellite phones, good watches, computers or cameras. The SIM circuit is part of the structure of a UICC that sometimes consists of PVC with embedded contacts and semi-conducers. SICs are a functional feature of a UICC. SIM cards between entirely separate mobile devices are transferable. The main excellent UICC cards were loan and bank cards dimensions; over the past years the dimensions have been decreased several times, usually with identical electrical contacts in order for a larger card to be bog-down to a lower one. A SIM card contains its distinctive serial number(ICCID), international mobile subscriber identity number (IMSI),security authentication and ciphering data , temporary data associated with the local networks, a listing of the services user has access to , and two passwords:

Revised Manuscript Received on August 05, 2019

Dr. Debabrata Sarddar, Department of Computer Science and Engineering, University of Kalyani, Kalyani, Nadia, W.B., India.

Utpal Ghosh, Department of Computer Science and Engineering, University of Kalyani, Kalyani, Nadia, W.B., India.

Rajat Pandit, Department of Computer Science, West Bengal State University, Barasat, W.B., India.

a personal identification number (PIN) for standard use and a personal unblocking code (PUC) is used in case of PIN unlocking.The SIM was at the beginning is introduced by the European Telecommunications Standards Institution in a detailed description of the design with the number TS 11.11.

1. External Structure

The external structure of a SIM is shown in fig. 1:

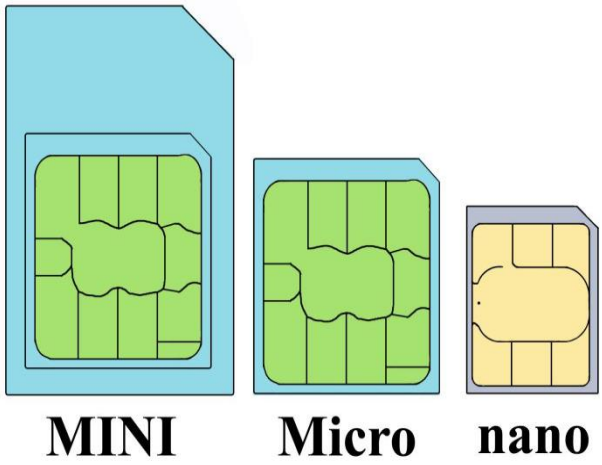


Fig. 1 : Subscriber Identification Module(SIM)

2. Internal Architecture

Internal architecture of a SIM card and it's circuit structure is shown in fig. 2 and fig. 3:

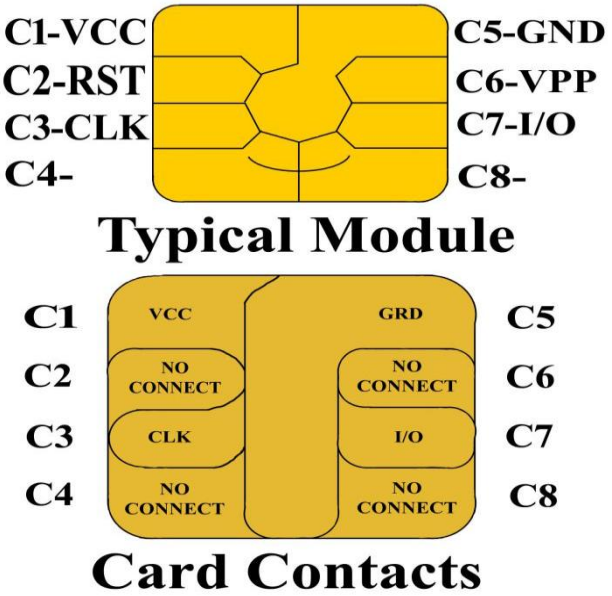


Fig. 2:General structure of SIM cards

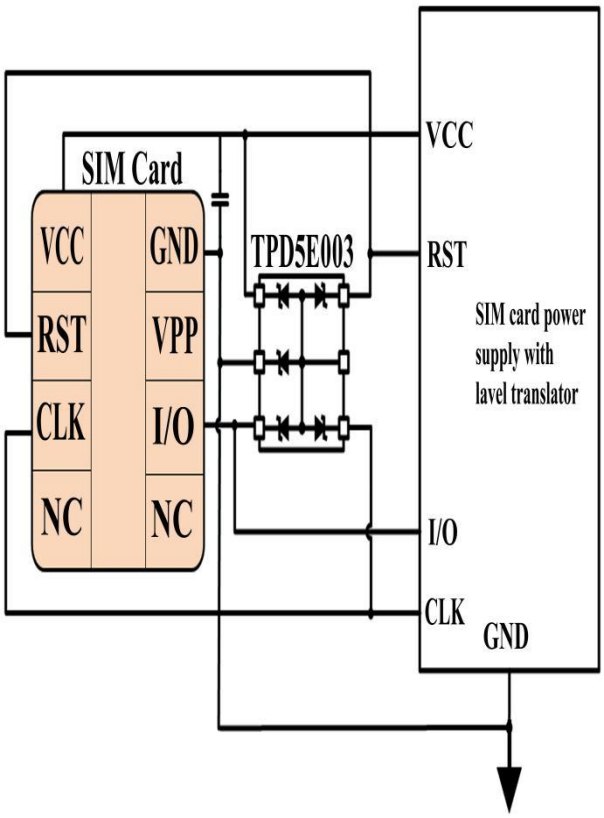


Fig. 3:Circuit diagram of a SIM card

The memory illustration structure is shown in fig. 4:

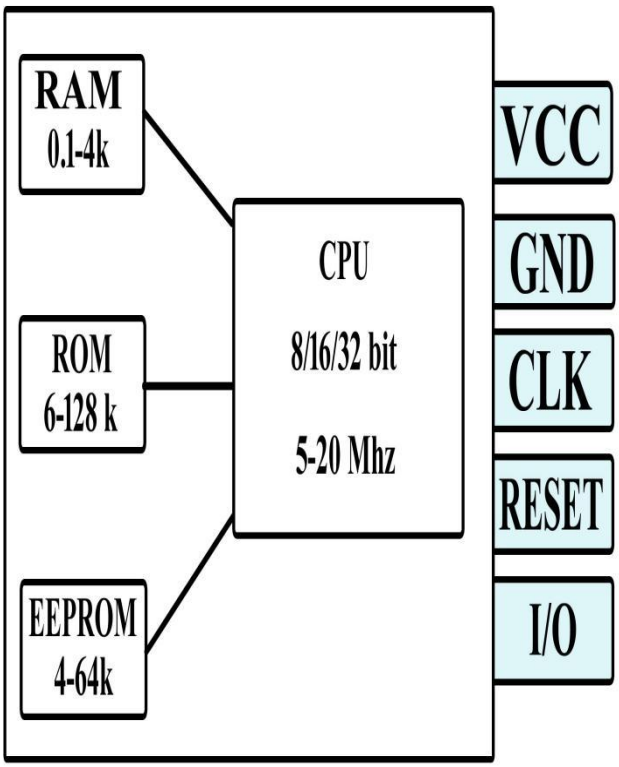


Fig. 4: Memory illustration of a SIM

3. Design of SIM

For SIM cards there are 3 operating voltages: 5V, 3V and 1. 8 V. Most of the SIM cards initiated before 1998 have operational voltage of 5V. Sequentially produced SIM cards are 3V and 1.8V compatible. The primary specifying conditions are specified as standard in the Instutution.They are as Follows:

ETSI TS 102 223
ETSI TS 102 241
ETSI TS 102 588
and
ETSI TS 131 111.

II. BIT FIELDS OF SIM CARD

SIM card storage Network — Centric information manipulated by and identified network subscribers. The main ones required are the ICCID, IMSI(International Mobile Subscriber Identity), Authentication Key(Ki) (Integrated Circuit Cards Identifier) and Local Identity(LAI) and the Operator-Specific emergency number. The SIM collects various carrier information like SMSC, SSN, Service provider number (SDN), to charge feedback parameters and value-added service (VAS) applications. Service dialing numbers (SADN) and VAS are the most common features of the SIM.

The network operator who issued the SIM card will use that to have a telephone connection to a well-liked network, which will be very cost effective for the provider instead of the client.

2.1. ICCID

ICCID is that the identifier of the particular SIM card itself that means it is act like as an identifier for the circuit chip of SIM . currently a days ICCID numbers are wont to determine eSIM profiles, and not solely physical SIM cards. every SIM is internationally known by its computer circuit card symbol (ICCID).IICIDs are keep within the SIM cards and conjointly incised or written on the SIM card body throughout a method called ‘personalization’. The ICCID is outlined by the ITU-T recommendation E.118 because the Primary Account number. The number consists of the subsequent sub parts. MII stands for Major industry identifier, that has 2 mounted digits, 89 for telecommunication functions. Country code 1 to 3 digits, as outlined by ITU-T recommendation E.164. Issuer identifier 1 to 4 digits. Its length is variable, however each number underneath one Issuer Identification Number(IIN) has the same length.

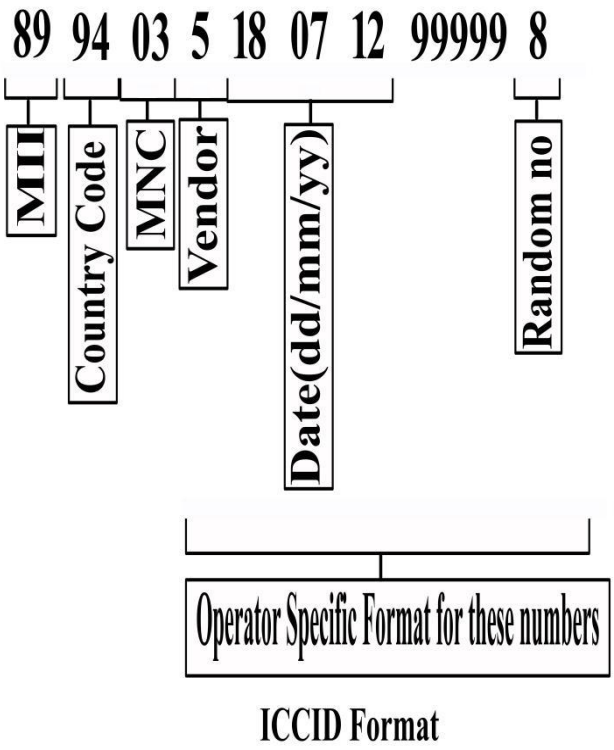


Fig. 5: The digit format of ICCID

2.1.1. Check digit of ICCID

A single digit calculated with the Luhn algorithm from the other digit. With a 10 octet GSM Section 1, the ICCID is maintained as a BCD packed, with 20 digits of space in the data field and the hex digit "F" as filter when necessary, as required. In follow, this means that on GSM SIM cards there are twenty digit (19+1) and 19-digit (18+1) ICCIDs in use, relying upon the establishment. However, one establishment continuously uses the identical size for its ICCIDs.

2.2. International Mobile Subscriber Identity(IMSI)

SIM cards are known on their individual operator networks by an unique International Mobile Subscriber Identity(IMSI). Mobile network operators connect portable calls and communicate with their market SIM cards exploitation their IMSIs. The bit format of IMSI is shown in fig. 6 and fig. 7:

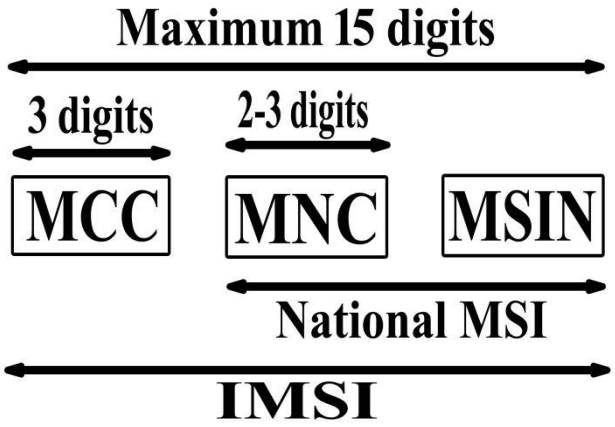


Fig. 6: Bit format of IMSI

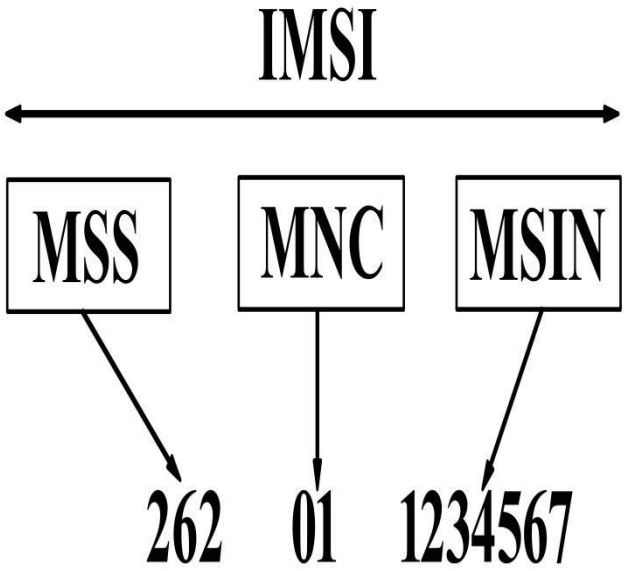


Fig. 7

2.3.Authentication key(Ki)

Every SIM holds a novel 128 bit Ki allotted to that by the operator throughout the personalization method for authenticating the SIMs on GSM.. The Ki is additionally keep in an exceedingly information on the network. The SIM card is intended to stop somebody from obtaining the Ki by using the smart-card interface.. In practice, the GSM cryptanalytic algorithm for computing SRES-2, which is mentioned within the following Authentication method.

2.3.1.Authentication Process

1. When the mobile tooling begins it receives the International Mobile Subscriber Identity (IMSI) on the SIM card and passes them on for correct access, authentication or validation, to the mobile service provider. Before this data is revealed, mobile devices might transfer a PIN to the SIM card.
2. The cellular service operator will then search for his own IMSI database and his associated Ki authentication key.
3. A random number(RAND) is then generated by the network operator and signed by Ki with the IMSI-connected, computing another number divided into the Signed Answer 1 (SRES_1, 32 bits) and also the Kc (64 bits) encoding key.
4. The RAND is sent to the mobile device and passed by the Operator Network to the SIM card. The SIM card signs it for the portable instrumentation with its Ki, producing SRES_ 2 and Kc. SRES_ 2 is transferred to the operator network via portable instrumentation.
5. The network of operators then compares its SRES_1 with the SRES_ 2 calculation that has retrieved mobile devices.. The two numbers will match the SIM and access to the operator's network also is allowed to mobile devices. Kc is used to encompass all additional communication between the mobile device and the network.

2.4. Location area Identity

The SIM stores information from the Location Area Identity (LAI) network. The new LAI values for the SIM are saved and returned to the mobile

service operators ' network connected to the new location, once the device changes locations.

2.5. SMS messages and contacts

Many SMS messages and phone book contacts are stored by SIM cards. It simply stores the contacts, which is **"name and number"** in pairing. Sometimes, numerous telephone numbers and additional telephone numbers do not appear on the SIM card. Early models have just 5 messages and 20 contacts stored, while trendy SIM cards can store over 250 contacts sometimes.

III. PROPOSED METHODOLOGY

Using of high memory SIM cards isn't new in any respect. however anytime with newer technology comes into the play the SIM card gets high memory bits. There are two SIM card sizes those are most well liked and presently being employed by most of the SIM card users: **A. 64 K SIM card**

B. 128 K SIM card

In our proposed work, though its named as **"Incrementing Bit Fields of SIM"** however we have a tendency to haven't set a selected size of SIM card but tried to convey general update to bit sizes employed by the predefined terms resides in bit fields. we have conjointly projected some way or series of steps (procedural work) to form a convenient or additional exactly a little step of our own to beat the "call drop" in modern-day. though ICCID doesn't would like an additional bits to store values as a result of it's already enough for unambiguously represent a SIM for over a mix of trillions. however still the protection are often raised by using additional higher cipher code generation Encryption-decryption strategies to attenuate the possibilities of SIM card swapping or cloning and different SIM hacking or fraud as a result of increased SIM memory have lots of space to run and store security algorithms.

So, for many value efficient result it is doubtless to possess additional preferred MSINs predefined by network operator. conjointly it saves the energy of the MS who is on the roaming currently and reduces further time interval. there is an issue in **'Automatic Network Selection'** , that is that 'Automatic Network Selection'

scans each single unit of time for opting the most effective MNC(Mobile Network Code). however the most effective in terms of what? as a result of it checks the signal strength of the radio signals it gets from a selected MNC. however it is not perpetually right, as a result of because the additional number of MS tries to attach with the identical MNC, it below flowed by the number of accessible channels and therefore leads to increasing wait time and even no signal in any respect.

On the opposite hand manual selection will get us a preferred network, however once the MS travels out of its radius the MS left with no alternative but 'Auto selection Mode'. to beat this drawback because it is hiking up day by day with- (a) Increasing number of SIM user and conjointly the internet. a brand new list of preferred networks to be embedded for home network selection likes as preferred networks for roaming. (b) Updates Regular basis. (c) Works in set of MNCs connects on day to day.

Here we have a tendency to proposed a brand new approach that named as **"Smart selection Mode"**

3.1. Algorithm

3.1.1. Makes a group of home MNCs connects in day to day.
3.1.2. Keeps record of attributes like 'Signal Strength', 'Internet Speed', 'Call drop'.
3.1.3. Orders or sorts the set of MNCs as per any attribute of alternative.
3.1.4. Selects the most effective result for home MNCs each time.
3.1.5. Updates the database on every occasion connects to the saved MNCs.

3.2. Flowchart of our Proposed Algorithm

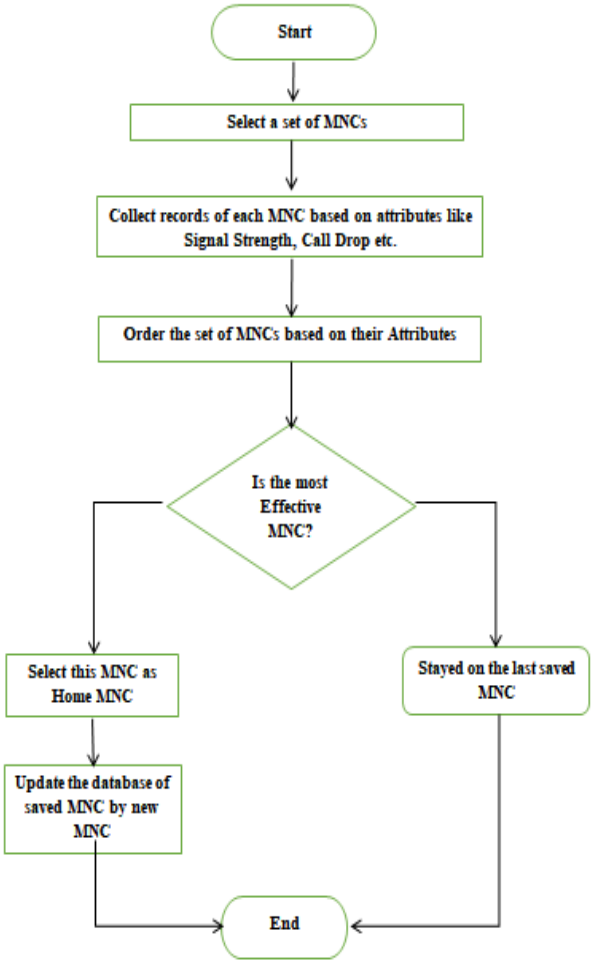


Fig. 8: Flowchart of Proposed Algorithm

3.3. Scope of the projected algorithm

As in currently, we tend to are within the new rise of wireless era wherever each product goes smart and obtaining connected with other by some radio signals. therefore in recent times a brand new term 'E-SIM' obtaining the place of trivial SIM cards. it is as sort of a SIM card however it is embedded within the product and can't be removed and conjointly it is not by a Network Service provider. So, it may be connected to any Network Service provider by their applications.So it is impracticable to offer all kind of preferred MNCs within the E-SIM for all Network Service provider. So, it may be unnoticed by either using database application or a wise preference making and updating procedure embedded into the hardware and our proposed

technique will the identical task as a second technique.

IV. RESULT ANALYSIS

The percentage of Effective MNCs is directly depended on the call drop probability. So, we can say that Effective MNC is inversely proportional to the Call Drop Probability. Fig. 9 shows the relationship between these:

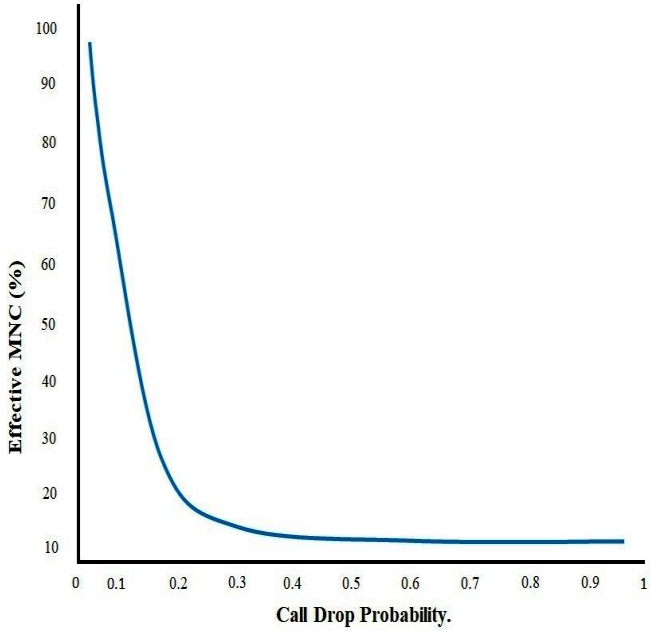


Fig 9: Effective MNC (%) vs. Call Drop Probability

Again, when we ordering the set of Effective MNC based on the signal strength, signal strength improving the the quality of MNC and provide the best MNC for service. So, when the signal strength is increased, the percentage of Effective MNC also increase i.e. signal strength is directly proportional to the Effective MNC. Fig 10 shows the relationship between them:

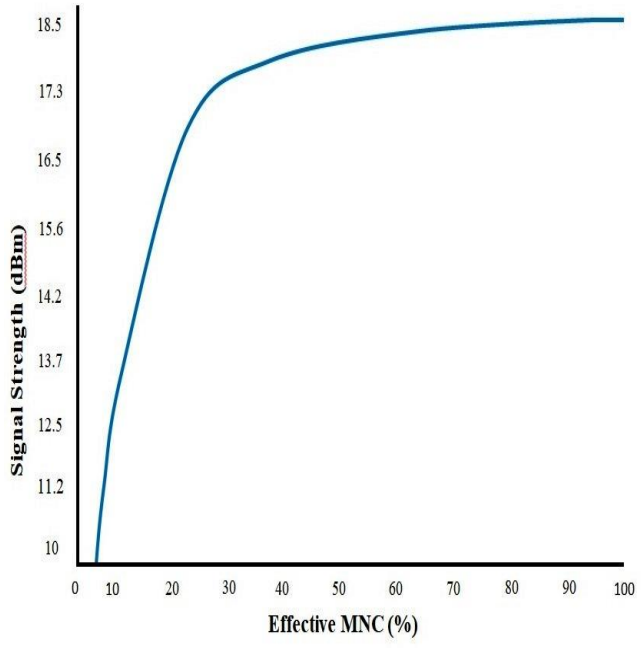
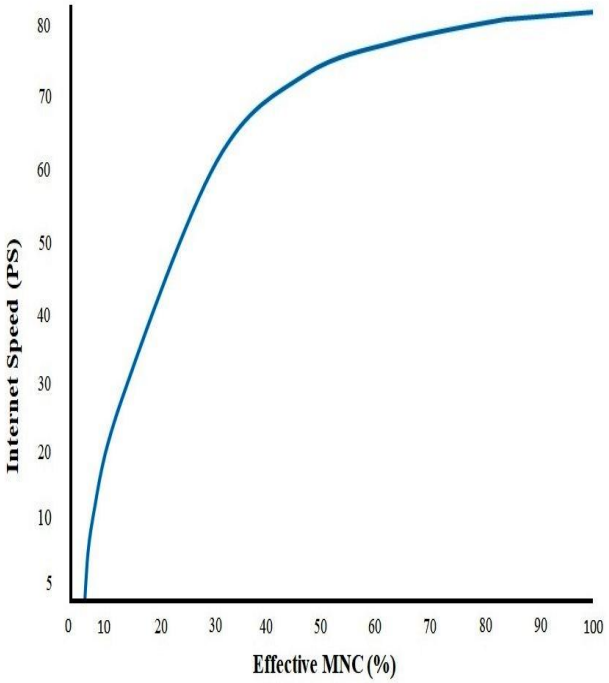


Fig 10: Signal Strength(dBm) vs Effective MNC(%)

And the last relation which is depends on both the Effective MNC and Signal Strength. When signal strength is provide best value, the most effective MNC is selected, and for rich signal strength the internet speed also increased. So, the percentage of effective MNC and the internet speed are also in directly proportional relation. Fig 11 shows the graphical relation between them:



V. CONCLUSION AND FUTURE IMPROVEMENT

Our proposed work evaluates a very small amount of potentialities within the whole world of SIM or Wireless technology to upgrade itself for higher results. however still there are several things in our work may be exhausted our next articles:

5.1. Use of SIMToolkit for Simulation.

5.2. practical comparison of our projected work with trivial ones.

ACKNOWLEDGEMENT

we would like to convey our hearty respect and sincerest feeling to our revered research adviser Dr. Debabrata Sarddar for sparing his valuable time and assimilating new flawless concepts at every stage of our work. without his kind co-operation, motivation, and careful steering, we might not have been able to perform this analysis work with success. we might additionally prefer to acknowledge DST-PURSE-II Programme for their kind co-operation.

REFERENCES

1. Casadei, Fabio, Antonio Savoldi, and Paolo Gubian. "Forensics and SIM cards: an Overview." International Journal of Digital Evidence 5.1 (2006): 1-21.
2. Vedder, Klaus. "Smart cards." 1992 Proceedings Computer Systems and Software Engineering. IEEE, 1992.

3. Jansen, Wayne, and Rick Ayers. "Forensic software tools for cell phone subscriber identity modules." Proceedings of the Conference on Digital Forensics, Security and Law. Association of Digital Forensics, Security and Law, 2006.
4. Haverinen, Henry, and Joseph Salowey "Extensible authentication protocol method for global system for mobile communications (GSM) subscriber identity modules (EAP-SIM)". No. RFC 4186. 2005.
5. Tsai, Yuh-Ren, and Cheng-Ju Chang. "SIM-based subscriber authentication mechanism for wireless local area networks." Computer communications 29.10 (2006): 1744-1753.
6. Tsai, Yuh-Ren, and Cheng-Ju Chang. "SIM-based subscriber authentication for wireless local area networks." IEEE 37th Annual 2003 International Carnahan Conference onSecurity Technology, 2003. Proceedings.. IEEE, 2003.
7. Urien, Pascal. "Convergent identity: Seamless OpenID services for 3G dongles using SSL enabled USIM smart cards." 2011 IEEE Consumer Communications and Networking Conference (CCNC). IEEE, 2011.
8. Rankl, Wolfgang, and Wolfgang Effing. Smart card handbook. John Wiley & Sons, 2004.
9. Joo, Jae Hyung, Jeong-Jun Suh, and Young Yong Kim. "Secure remote USIM (Universal Subscriber Identity Module) card application management protocol for W-CDMA networks." 2006 Digest of Technical Papers International Conference on Consumer Electronics. IEEE, 2006.
10. ZHOU, Jienan, Jianghong SHI, and Hong WANG. "Research and Design on Subscriber Identity Module Reader [J]." Modern Electronics Technique 8 2007.

AUTHOR'S BIBLIOGRAPHY

Dr. Debabrata Sarddar, Assistant Professor in the Department of Computer Science and Engineering, University of Kalyani, Kalyani, Nadia, West Bengal, INDIA. He has done Ph.D. at Jadavpur University.He completed his M.Tech in Computer Science & Engineering from DAVV, Indore in 2006, and his B.E in Computer Science & Engineering from NIT, Durgapur in 2001. He has published around 200 research papers in different journals, attend 50 conferences, wrote 10 Book Chapters and 3 books. His research interest includes wireless and mobile system, Cloud Computing and Wireless Sensor Network.

Mr. Utpal Ghosh is presently pursuing M.Tech in Computer Science and Engineering at the Department of Computer Science and Engineering, University of Kalyani, Kalyani, Nadia, West Bengal, India. He has completed his MCA from Department of Computer Science and Engineering, University of Kalyani, Kalyani, Nadia, West Bengal, India in 2017. His research interest includes Mobile Computing, Wireless Sensor Network and Cloud Computing.

Mr. Rajat Pandit is an assistant professor in the Department of Computer Science, West Bengal State University, West Bengal, India. He has completed his M.Tech (IT) from West Bengal University of Technology, West Bengal, India in 2009. He has completed his MCA from Jadavpur University, West Bengal, India in 2001. His research interest includes Mobile Computing, Wireless Sensor Network and Cloud Computing.