-: Mobile IP in GSM Architecture :-

Aim:- To study how the mobile IP is used in GSM architecture.

Abstract:-

The international operation of a GSM system includes among others the interoperability with other GSM networks (including different countries) and with ISDN networks, as well as the information exchange among network operators (billing, statistical data, subscriber complaints, invalid IMEI etc.).This case study will highlight the emergence of GSM over the 1G: Analog Cellular Networks.

Keywords: - GSM, Mobile IP, foreign agent, home agents.

Introduction:-

Cellular communication means that there are a lot of different areas, looks like cell, contain communication system devices, such as antennas, base stations. If the base station antenna power is high, it means that it serves large areas.

Otherwise, if the antenna power is low, it means that it serves little areas. However there are other parameters which affect the convergence. For example, to achieve a good communication in crowded areas, convergence should be reduced and the channel capacity should be increased.

A lot of adjacent cells create the clusters.

Clusters can have different amount of cells and each cell uses different frequency to avoid interference. These cluster structures repeat itself in different communication areas.

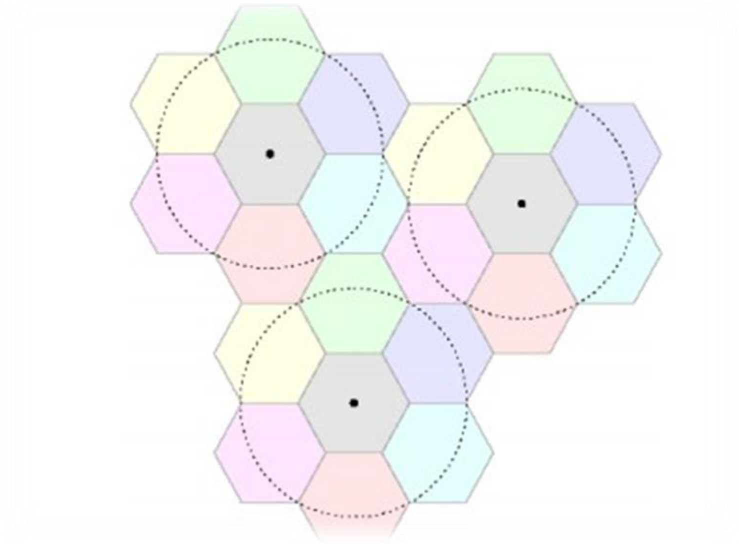

Fig 1 Cell and Cluster Structures
Courtesy: http://www.radio-electronics.com

Mobile IP

Shows a generic Mobile IP network. The mobile device attaches to a network through a router that terminates a radio interface1. Inside the network there are two mobility agents: a home agent and a foreign agent. Each mobile node has two addresses assigned to it. A home address that corresponds to its home network and a care-of address that corresponds to the network to which it is currently attached. When a mobile device attaches to a network, it receives a care-of address from the serving network.

This is often the address of an interface on the foreign agent serving the mobile device. The mobile device then registers this address with its home agent. Mobile security associations are required between the mobile device and its home agent. In addition, further security associations may exist between the mobile device and the foreign agent, and the foreign and home agents.

When packets are sent to the mobile device by a corresponding host, they are addressed to the home address of the mobile node. These packets are routed through the Internet as normal IP packets until they reach the home network of the mobile device.

In the home network, the home agent of the mobile device intercepts these packets. The home agent encapsulates these packets inside packets that are addressed to the care-of address of the mobile device. These packets are then routed on the Internet as normal IP packets until they reach the foreign agent corresponding to the mobile device.

In this way packets are tunneled through the network. The foreign agent decapsulates the original IP packets and forwards them to the mobile device. Packets sent from the mobile device may be treated as normal IP packets.

When a mobile device moves between points of attachment on a network and changes foreign agent, it receives a new care-of address, and re-registers with its home agent. In this way, mobility management is performed. Mobile IP also defines mechanisms allowing mobile devices to perform their own decapsulation functions, by means of a co-located care-of address.

In addition, the IETF is working on an extension to Mobile IP called route optimization [8], allowing the home agent to inform corresponding hosts about the current care-of address of mobile devices. Route optimization also allows packets to be forwarded from an old foreign agent to a new foreign agent, enabling smoother handoffs.

Mobile IP in GSM Architecture

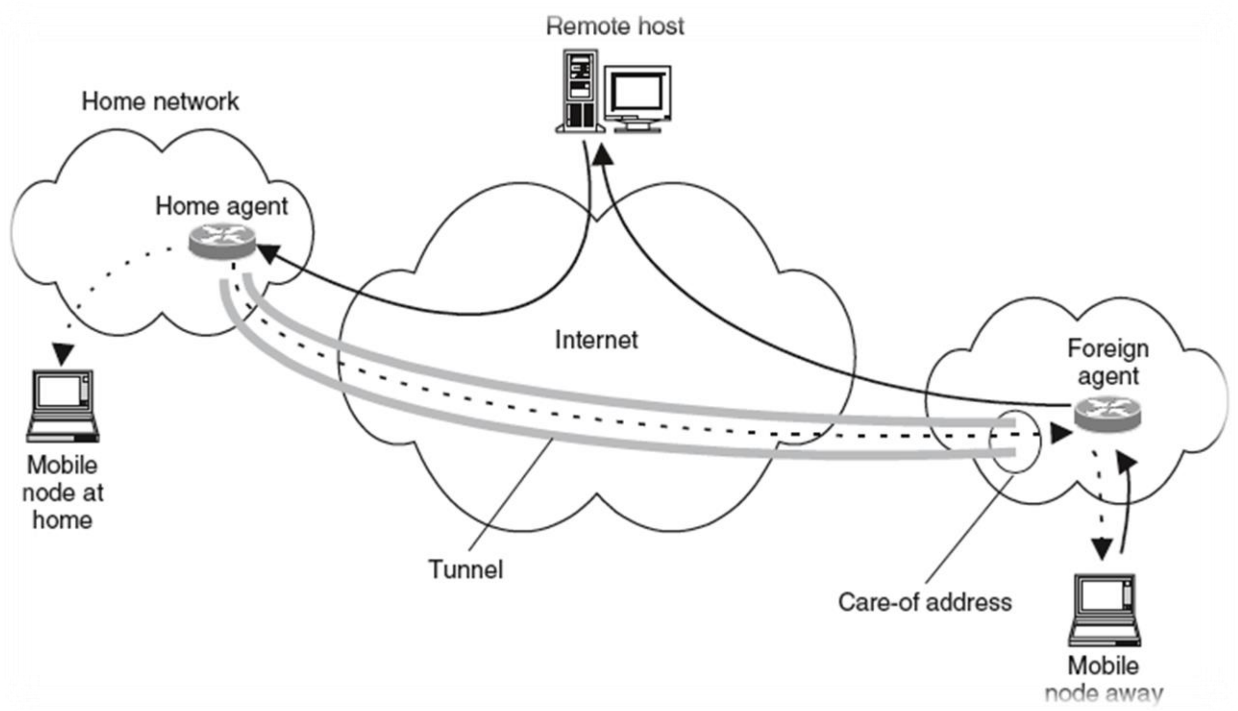

Fig 2 Mobile IP Network.

GSM, the Global System for Mobile communications, is a digital cellular communications system that has rapidly gained acceptance and market share worldwide. In addition to digital transmission, GSM comprises many advanced services and features, including ISDN

(Integrated Services Digital Network) compatibility and worldwide roaming in other GSM networks. GSM architecture is a combination of three subsystems: Base Station Subsystem (BSS), Network Switching Subsystem (NSS) & Operation Support Subsystem (OSS).

BSS consists of Base Transceiver System (BTS) and Base System Controller (BSC) which connects with Mobile Station (MS). NSS consists of MSC which connects with BSC. OSS maintains BSS and NSS.

GSM channels are responsible for connecting two MS's. It consists of two channels: Traffic Channels (TCH) which makes data flow between two MS's possible and Control Channels (CCH) which supervises the signaling and synchronization between the base station and mobile station. This paper will give an overview of GSM system architecture & its channels.

GSM:

The development of Global System for Mobile Communication (GSM) started in 1982 when the Conference of European Posts and Telegraphs (CEPT) formed a study group called Grouped Special Mobile (the initial meaning of GSM) whose aim was to study and develop a pan-European public cellular system in the 900 MHz range [6]. Some of the basic criteria for their proposed system were:

- Good subjective speech quality
- Low terminal and service cost

- Support for international roaming
- Ability to support handheld terminals
- Support for range of new services and facilities
- Spectral efficiency
- ISDN compatibility

GSM uses a mixture of both Frequency Division Multiple Access (FDMA) and Time Division Multiple Access (TDMA). FDMA parts include the division by frequency of the 25 MHz bandwidth into 124 carrier frequencies spaced 200 KHz for GSM900. TDMA further divides each carrier frequencies into 8-time slots such that

each carrier frequency is shared by 8 users. In GSM, the basic radio resource is a time slot with duration of 577 µs. 8 Time slots of 577 µs constitute a 4.615 ms TDMA Frame. GSM uses Gaussian Minimum Shift Keying (GMSK) modulation scheme to transmit information over Air Interface. GSM uses number of channels to carry data over air interface; these channels are

Broadly divided into following two categories:
i. Physical Channels
ii. Logical Channels

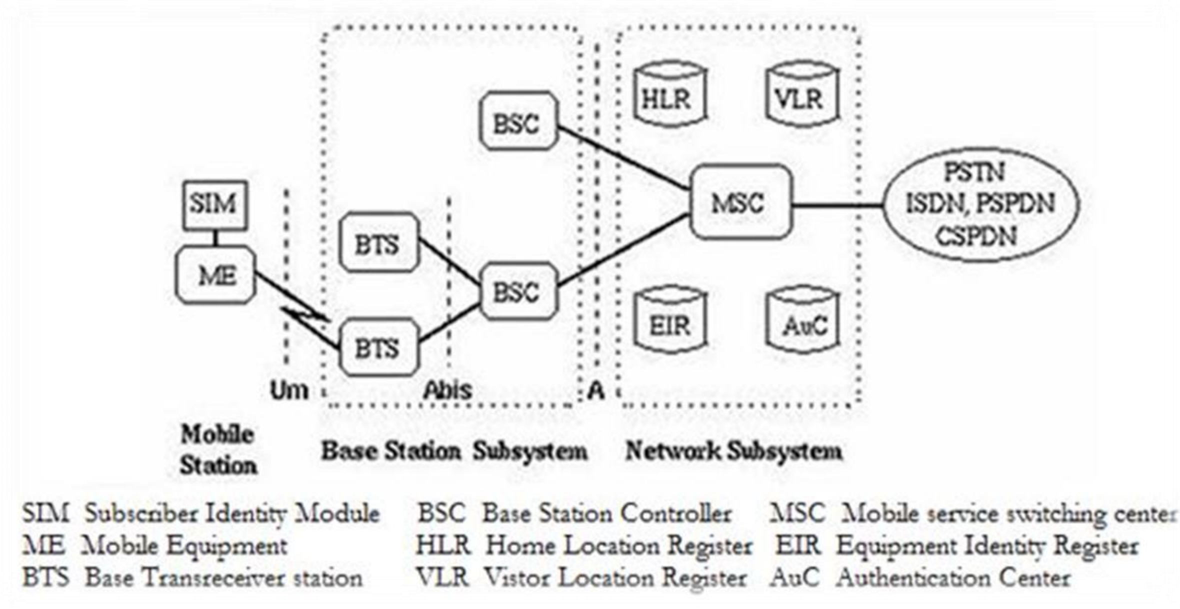
SIM
ME
BTS
BTS
BSC
BSC
HLR
VLR
MSC
EIR
AuC
PSTN
ISDN, PSPDN
CSPDN
Um
Abis
A
Mobile Station
Base Station Subsystem
Network Subsystem
SIM Subscriber Identity Module
ME Mobile Equipment
BTS Base Transreceiver station
BSC Base Station Controller
HLR Home Location Register
VLR Vistor Location Register
MSC Mobile service switching center
EIR Equipment Identity Register
AuC Authentication Center

Fig 3 GSM Architecture

- The GSM network architecture consists of three major subsystems:
- Mobile Station (MS)
- Base Station Subsystem (BSS)
- Network and Switching Subsystem (NSS)
- The wireless link interface between the MS and the Base Transceiver Station (BTS), which is a part of BSS. Many BTSs are controlled by a Base Station Controller (BSC). BSC is connected to the Mobile Switching Center (MSC), which is a part of NSS. Figure shows the key functional elements in the GSM network architecture.

1. Mobile Station (MS):

A mobile station communicates across the air interface with a base station transceiver in the same cell in which the mobile subscriber unit is located. The MS communicates the information with the user and modifies it to the transmission protocols if the air-interface to communicate with the BSS.

The user's voice information is interfaced with the MS through a microphone and speaker for the speech, keypad, and display for short messaging, and the cable connection for other data terminals. The MS has two elements.

The Mobile Equipment (ME) refers to the physical device, which comprises of transceiver, digital signal processors, and the antenna. The second element of the MS is the GSM is the Subscriber Identity Module (SIM). The SIM card is unique to the GSM system. It has a memory of 32 KB.

2. Base Station Subsystem (BSS):

A base station subsystem consists of a base station controller and one or more base transceiver station. Each Base Transceiver Station defines a single cell. A cell can have a radius of between 100m to 35km, depending on the environment.

A Base Station Controller may be connected with a BTS. It may control multiple BTS units and hence multiple cells. There are two main architectural elements in the BSS – the Base Transceiver Subsystem (BTS) and the Base Station Controller (BSC).

The interface that connects a BTS to a BSC is called the A-bis interface. The interface between the BSC and the MSC is called the A interface, which is standardised within GSM.

3. Network and switching subsystem (NSS)

The NSS is responsible for the network operation. It provides the link between the cellular network and the Public switched telecommunicates Networks (PSTN or ISDN or Data Networks). The NSS controls handoffs between cells in different BSSs, authenticates user and validates their accounts, and includes functions for enabling worldwide roaming of mobile subscribers. In particular the switching subsystem consists of:

- Mobile switch center (MSC)
- Home location register (HLR)
- Visitor location Register (VLR)
- Authentications center (Auc)
- Equipment Identity Register (EIR)
- Interworking Functions (IWF)

The NSS has one hardware, Mobile switching center and four software database element: Home location register (HLR), Visitor location Register (VLR), Authentications center (Auc) and Equipment Identity Register (EIR). The MSC basically performs the switching function of the system by controlling calls to and from other telephone and data systems. It includes functions such as network interfacing and common channel signaling.

HLR:

The HLR is database software that handles the management of the mobile subscriber account. It stores the subscriber address, service type, current locations, forwarding address, authentication/ciphering keys, and billings information.

In addition to the ISDN telephone number for the terminal, the SIM card is identified with an International Mobile Subscribes Identity (IMSI) number that is totally different from the ISDN telephone number. The HLR is the reference database that permanently stores data related to subscribers, including subscriber's service profile, location information, and activity status.

VLR:

The VLR is temporary database software similar to the HLR identifying the mobile subscribers visiting inside the coverage area of an MSC. The VLR assigns a Temporary mobile subscriber Identity (TMSI) that is used to avoid using IMSI on the air.

The visitor location register maintains information about mobile subscriber that is currently physically in the range covered by the switching center. When a mobile subscriber roams from one LA (Local Area) to another, current location is automatically updated in the VLR.

When a mobile station roams into anew MSC area, if the old and new LA's are under the control of two different VLRs, the VLR connected to the MSC will request data about the mobile stations from the HLR. The entry on the old VLR is deleted and an entry is created in the new VLR by copying the database from the HLR.

AuC:

The AuC database holds different algorithms that are used for authentication and encryptions of the mobile subscribers that verify the mobile user's identity and ensure the confidentiality of each call. The AuC holds the authentication and encryption keys for all the subscribers in both the home and visitor location register.

EIR:

The EIR is another database that keeps the information about the identity of mobile equipment such the International mobile Equipment Identity (IMEI) that reveals the details about the manufacturer, country of production, and device type. This information is used to prevent calls from being misused, to prevent unauthorized or defective MSs, to report stolen mobile phones or check if the mobile phone is operating according to the specification of its type.

White list:

This list contains the IMEI of the phones who are allowed to enter in the network.

Black list:

This list on the contrary contains the IMEI of the phones who are not allowed to enter in the network, for example because they are stolen.

Grey list:

This list contains the IMEI of the phones momentarily not allowed to enter in the network, for example because the software version is too old or because they are in repair.

IWF(Inter Working Function):

It is a system in the PLMN that allows for non speech communication between the GSM and the other networks. The tasks of an IWF are particularly to adapt transmission parameters and protocol conversions.

The physical manifestations of an IWF may be through a modem which is activated by the MSC dependent on the bearer service and the destination network. The OSS (Operational Support Systems) supports operation and maintenance of the system and allows engineers to monitor, diagnose, and troubleshoot every aspect of the GSM network.

Study Parts:-

In this section we discuss how the mobility management procedures of Mobile IP may work in a GSM network. We consider four issues with mobility management: detecting a change in network attachment, micro mobility, paging, and roaming.

1. Change in Network Attachment:

Mobile IP defines two methods for determining that a change in network attachment has occurred, thus triggering procedures to obtain a new care-of address and re-register with a home agent. In the first, foreign agents broadcast Foreign Agent Advertisements, which are received by the mobile devices on the same subnet as the foreign agent.

These advertisements include the care-of addresses supported by the foreign agent. Through a set of well-defined rules, a mobile device can deduce when it is no longer in contact with its existing foreign agent and must therefore register with a new foreign agent. In the second method, when a mobile device senses a change in link level attachment to a network, it searches for a suitable foreign agent on the new subnet, or over the air interface, by sending Foreign Agent Solicitation messages to which any receiving foreign agent may reply.

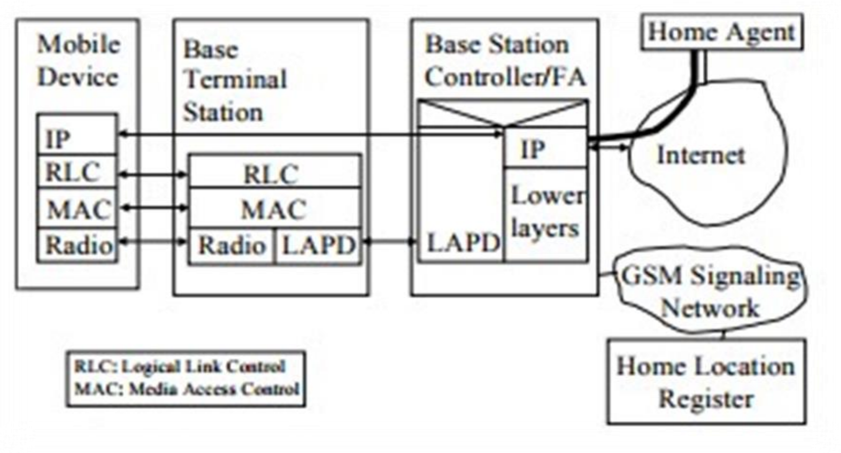

Fig 4 Reference system

The agent advertisement is convenient when a broadcast channel is present. All cellular air interfaces have broadcast channels defined. However, they are of limited capacity and support only standard messages3. Unless a change is effected in the standards, these channels cannot be used to broadcast agent advertisements.

A possible solution is to have the mobile device acquire a link level connection to the network, and then have the foreign agent multicast agent advertisements to all connected users. This technique simulates a broadcast network. The drawback of this approach is the overhead of multicasting the agent advertisements.

Alternatively, when a mobile device determines it has changed base stations by virtue of the standard broadcast channels, it may send an agent solicitation message on the link. This will be received by the foreign agent which may then reply with a care-of address. This technique is simple and does not require updates to any standards. Also, it will work with any air interface.

B. Micro mobility

Once a change in network attachment is detected, a handoff (known as a mobility update in GPRS) must occur for the mobile device to continue to receive data. To do this, routing tables, or their equivalents, must be updated in the network.

In a pure Mobile IP network, all mobility may be handled at the IP level. In a cellular network, as shown in Fig. 3, mobility between two BTS' on a common BSC cannot be handled at the IP level because the BTS' are not assigned IP addresses and are not IP routers.

In a BSC, a mapping exists between the IP address of the mobile device, the link layer connection to the BTS and the air interface connection with the mobile device. To perform a handoff requires mapping packets arriving at the FA to a different outgoing link to a BTS.

Therefore, there are two levels at which handoffs must be handled. At the lowest level, link level mobility is provided; above this, IP level mobility is provided.

C. Paging

In Mobile IP networks, because the network is IP end-to-end, a mobile device is always reachable. If the device moves to a different point in the network, its care-of IP address changes, and it re-registers.

In a cellular network, registrations from a mobile device do not typically occur upon each move unless a logical boundary or some pre-defined level in the network hierarchy is crossed. Therefore, there are periods when the exact location of a mobile device is unknown beyond a certain level in the network.

This is done purposefully so that mobile devices may enter a standby mode to conserve power and do not have to reregister with the network frequently. When a device must be located, and its location is not precisely known, the network pages over the air interface for the device. When the device responds, its exact location is determined, routing tables are updated, and packets are delivered.

One simple solution to interworking paging in a cellular network is to place the FA at the BSC as shown in Fig. 4. When the mobile device moves between BSCs, it receives a new care-of address and registers. In this way, the network can always route packets to the current BSC serving the mobile device.

When packets arrive at the BSC, if it does not have a current mapping for the device, the BSC pages the mobile device to locate its current BTS. When the device responds, the BSC updates its tables, and forwards packets to the mobile device. This requires that the BSC queue packets for the mobile device while the paging procedure is executing.

An alternative solution is for the BSC to broadcast packets for the mobile device to all of its BTS' if it does not know the exact BTS serving the mobile device. When the mobile device receives the first packet, it will respond and allow the BSC to update its tables and unicast subsequent packets. This eliminates the need for queuing at the BSC, but increases the air interface usage.

D. Roaming

In a cellular network, when a mobile device moves between logical registrations areas, it registers with its VLR and HLR. This allows the mobile device to be located by other corresponding users. To locate a mobile device, the HLR is queried, which in turn queries the VLR, which responds with the location of the mobile device. The logical registration areas may cover several BSCs.

The HLR is assigned based on the GSM address of the mobile device. It is not a router, and does not receive or process user data. As discussed in Section IV, it plays a key role in authenticating the mobile device. In a Mobile IP network, similar functions are managed by interactions between the FA and HA.

The FA replaces the functionality of a VLR; it receives local registration messages, and if a new mobile registers, it contacts the home agent to register the mobile device. The HA, like the HLR, knows the foreign agent currently serving the mobile device.

Unlike the HLR, the HA receives all data packets destined to the mobile device and can forward them directly to the correct FA. Therefore, for data routing functions, the HA may replace the HLR. However, as we discuss in Section IV, the HLR is also used to perform additional security functions in GSM.

SECURITY

There are two aspects to security in a wireless system: authenticating users and approving them for service, and encrypting user information and signaling to prevent eavesdropping.

A. Authentication

In a GSM network, a mobile device and its HLR share a secret key. When a mobile device registers with a VLR for the first time, the VLR contacts the HLR to request authentication information for the user. The HLR replies with a set of random numbers and their corresponding signatures computed using the secret key of the mobile. The VLR can then challenge the mobile with one of the random numbers.

The mobile uses its secret key to compute the signature of the random number, and sends the result back to the VLR. The VLR authenticates the mobile by matching its reply with the signature loaded by the HLR. While the HLR and the mobile device share a permanent security association (the secret key), the VLR and the mobile device share a temporary security association (the set of random numbers and their associated signatures).

In a Mobile IP system, each mobile device shares a secret key with its home agent. Optionally, a mobile can share a different secret key with each foreign agent, and each foreign agent can share another key with the home agent.

Each registration message and the associated reply contain a set of authentication extensions, computed by signing the message with the relevant secret key. For example, the home agent can authenticate a message coming from a mobile by computing the signature of the message with the key it shares with the mobile, and comparing the result with the signature contained in the authentication extension.

One of the issues associated with this authentication technique is the burden in distributing the set of authentication keys. Ongoing work in the IETF [9] proposes using three sets of short-lived authentication keys that would be distributed to the HA, FA, and mobile by an Authentication, Authorization, and Accounting (AAA) server.

In this case the AAA server, similar to an HLR, would share the permanent secret key with the mobile, while the three set of temporary keys would be used for authentication between mobile and FA, FA and HA, and mobile and HA.

As with GSM, the mobile would hold a permanent security association with the AAA server, while temporary security associations would exist between the mobile, the foreign agent, and the home agent.

One option for using Mobile IP in a cellular network is to retain both authentication procedures. The HLR/VLR would authenticate based on the GSM address of the device, and the AAA/HA/FA would authenticate based on the IP address of the device. The drawback of this approach is the extra overhead.

A second option is to have the HLR act as the AAA server. In this case, the permanent secret key shared between the HLR and the mobile device would be the same for the Mobile IP and GSM authentication. To implement this approach, the HLR would have to be augmented with an IP interface so that it could distribute to HAs and FAs the set of short-lived keys used for Mobile IP authentication.

For example, a FA acting as a VLR would receive from the HLR a set of temporary authentication keys, derived from the mobile's secret key and a set of random numbers. The set of authentication keys could then be used to perform Mobile IP authentication between the mobile device and the FA using standard authentication extensions.

B. Ciphering

In GSM, along with the random numbers and corresponding signatures, the HLR loads the VLR with a series of temporary ciphering keys that may be used by the mobile device. These ciphering keys may be computed only using the mobile's secret key over the random numbers.

Therefore, when ciphering is to be enabled, the VLR sends the mobile device one of the random values it received from the HLR along with the ciphering algorithm selected by the HLR.

The mobile device computes the ciphering key from its secret key and the random number and uses it for ciphering both user data and signaling on the session.

Although Mobile IP does not provide any encryption service per se, the IETF is defining a mechanism to enable the use of IPSec [10] ciphering tunnels with Mobile IP [11]. For example, while Mobile IP tunnels provide basic IP connectivity to the mobile, the establishment of IPSec tunnels between the mobile and the HA would enable the ciphering of the data.

Mechanisms are being defined for establishing IPSec tunnels between mobile and HA, FA and HA, or mobile and FA. As in GSM, the keys used for ciphering are different from the keys used for authentication. Ciphering keys are distributed to the interested parties by means of standard IPSec procedures during the setup of the tunnel.

Mobile IP in GSM Architecture

In the case of Mobile IP in cellular networks, the GSM and IPSec ciphering systems could be applied independently from each other, using two different sets of ciphering keys. This approach could be expensive, both because of the burden in maintaining two separate sets of ciphering keys, and because of the overhead of the two encryption systems running in parallel.

An alternative approach would be to use the same set of temporary ciphering keys distributed by the HLR to activate IPSec tunnels, and to selectively enable one encryption mechanism or the other in different parts of the network.

For example, where the air interface provides a limited bandwidth, GSM encryption could be used between the mobile device and the foreign agent, while an IPSec tunnel would serve the purpose between the FA and the HA. On the other hand, if the mobile decided to enable IPSec encryption with its home agent, GSM encryption on user data should be disabled.

Analysis:-

CDMA (Code-Division Multiple Access) refers to any of several protocols used in second-generation (2G) and third-generation (3G) wireless communications. As the term implies, CDMA is a form of multiplexing, which allows numerous signals to occupy a single transmission channel, optimizing the use of available bandwidth. The technology is used in ultra-high-frequency (UHF) cellular telephone systems in the 800-MHz and 1.9-GHz bands.

Table 1 CDMA Vs. GSM

	CDMA	**GSM**
Stands for	Code Division Multiple Access	Global System for Mobile communication
Storage Type	Internal Memory	SIM (subscriber identity module) Card
Data transfer	EVDO/3G/4G/LTE	GPRS/E/3G/4G/LTE
Network	There is one physical channel and a special code for every device in the coverage network. Using this code, the signal of the device is multiplexed, and the same physical channel is used to send the signal.	Every cell has a corresponding network tower, which serves the mobile phones in that cellular area.

International roaming	Less Accessible	Most Accessible
Frequency band	Single (850 MHz)	Multiple (850/900/1800/1900 MHz)
Network service	Handset specific	SIM specific. User has option to select handset of his choice.

Conclusion:-

The communication development and the increase of living standard of people are directly related to the more use of cellular mobile. Cellular mobile radio-the high end sophisticated technology that enables everyone to communicate anywhere with anybody. The mobile telephony industry rapidly growing and that has become backbone for business success and efficiency and a part of modern lifestyles all over the world.

In this case study we have tried to give and over view of the GSM system. We hope that we gave the general flavor of GSM and the philosophy behind its design. The GSM is standard that insures interoperability without stifling competition and innovation among the suppliers to the benefit of the public both in terms of cost and service quality.

The features and benefits expected in the GSM systems are superior speech quality, low terminal, operational and service costs, a high level security, providing international roaming support of low power hand portable terminals and variety of new services and network facilities. In near forth coming days, the third generation mobile telephony becomes available whole over the world, which will give the facility of videoconference in mobile telephone.

Future Enhancement:-

- Many of the GSM technologies are patented by Qualcomm and hence licenses need to be obtained from them.
- In order to increase the coverage repeaters are required to be installed.
  GSM provides limited data rate capability, for higher data rate GSM advanced version devices are used.
- GSM uses FTDMA (**Frequency division multiple access**) access scheme. Here multiple users share same bandwidth and hence will lead to interference when more number of users are using the GSM service. In order to avoid this situation, robust frequency correction algorithms are used in mobile phones and base stations.
- *Robust frequency correction algorithms*

GSM/GPRS uses a combination of FDMA and TDMA. A frequency correction burst (FCH burst) and synchronization burst are used in the acquisition phase of frequency and timing synchronization, respectively, by the mobile station (MS). A prior knowledge of timing is required for the MS to capture the FCH burst.

Timing sync algorithm cannot be used to get timing information unless frequency sync is achieved. So there is it need to identify the time of occurrence of the FCH burst before timing acquisition is achieved. In this paper, we proposed a robust algorithm that exploits the properties of the FCH burst to identify its location accurately enough to perform frequency sync.

The convergence property of an adaptive line enhancer (ALE) in the FCH burst is used for detection of the FCH burst and the divergence property of the ALE at FCH burst transition is used to identify the edges of the FCH burst.

Some simulation results are illustrated to show the effectiveness of the proposed algorithm. The algorithm is robust enough to perform well even for large frequency mismatches between MS and base station and low SNRs. The algorithm is computationally efficient without sacrificing performance.

References:-

1. La Porta, T.F., Salgarelli, L. and Foster, G.T., 1999. Mobile IP and wide area wireless data. In *Wireless Communications and Networking Conference, 1999. WCNC. 1999 IEEE* (Vol. 3, pp. 1528-1532). IEEE.
2. Digital Cellular Telecommunication System, General Packet Radio Service (GSM 02.60, version 6.1), ETSI, 1997.
3. Digital Cellular Telecommunication System, Enhanced Data Rates for GSM Evolution - Project Plan and Open Issues for EDGE (GSM 10.59, version 1.6), ETSI, 1997.
4. C. E. Perkins, “IP Mobility Support,” IETF RFC 2002, October 1996.
5. Digital Cellular Telecommunication System, Network Architecture (GSM 3.02, version 6.1), ETSI, 1997.
6. 800 MHz TDMA Cellular Radio Interface – Mobile Station – Base Station Compatibility, EIA/TIA IS-136, 1994
7. Mobile Station – Base Station Compatibility Standard for Dual-Mode Wide Band Spread Spectrum Cellular System, EIA/TIA IS-95, 1993.
8. IEEE Personal Communications Magazine Special Issue, “Third Generation Mobile Systems in Europe,” Davide Grillo Guest Editor, Vol. 5, No. 2, April, 1998.
9. C. E. Perkins, D. Johnson, “Route Optimizations for Mobile IP,” Internet Draft, November, 1997.
10. P. Calhoun and C. E. Perkins, DIAMETER Mobile IP Extensions, Internet Draft, November 1998.
11. S. Kent and R. Atkinson, Security Architecture for the Internet Protocol, IETF RFC 2401, November 1998.
12. J. K. Zao and M. Condell, Use of IPSec in Mobile IP, Internet Draft, November 1997.