International Journal of Engineering Science Invention
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org Volume 3 Issue 5ǁ May 2014 ǁ PP.01-11

Wireless Cellular Security Mechanism

[1,]Ashish Kumar, [2,]Yashlok Kumar , [3,]Deepak Kumar,
[1,]IT Analyst (Tata Consultancy Services), M-Tech (ECE), Manav Bharti University, HP.
[2,]M-Tech (ECE), Manav Bharti University, HP.
[3,]Scientist (ISRO), MS (Micro-Electronics), Manipal University.

ABSTRACT : *Mobile and Wireless technologies have evolved beyond recognition when the first radio signal was transmitted by pioneers like Nikola Tesla in the late nineteenth century. Since then Radio waves have been used as basis of telephony, audio & video broadcast and in radar system. Thus it is utmost vital to provide a safe and secure channel to user for communication.Topic covered under this paper will cover brief of cellular network, their architecture, security issue and mechanism to depecit it through wireless Application Protocol (WAP) & new 3G Cellular Network Architecture. Accordingly, through this paper we survey issues and dilemma in enhancing the survivability of mobile wireless network through designing of end to end communication in different environments where path from source to destination is not available at any given instant of time.*

KEYWORDS : *Wi-Fi, Cellular Network, Survivability, weak and episodic connectivity, ad hoc routing, Low probability for communication (LPC), fault tolerance, Authentication Authorization Accounting (AAA), Wireless Application Protocol.*

I. INTRODUCTION

Cellular Communication has become an important part of our daily life. Besides using cell phones for voice Communication, we are now able to access the Internet, conduct monetary transactions etc. However wireless medium has certain limitations over wired medium such as open access, limited bandwidth and systems complexity. The certain generation of 3G networks has a packet switched core which is connected to external network such as the internet making it vulnerable to new type of attacks such as denial of service,virus, worms etc. that have been used against the Internet . In wireless data communication at the beginning of 21stcentury, there observe a real explosion of wireless data communication with wireless LAN (WLAN, IEEE802.11), Personal area network (PANs such as Bluetooth or IEEE 802.15, Zigbee or IEEE802.15.4 or IEEE802.15.4a) and wireless metropolitan area network (WiMAX or IEEE802.16). All these technologies have been introduced with cryptographic security from beginning, even if the solutions are far from robust. In addition, mobile data communication is growing on the evolving GSM mobile phones using technologies such as GPRS and EDGE as on the third generation mobile phones such as 3GSM.For voice communication, introduction of security has been slower due to technological limitation and legal barrier since government want to maintain the capability to perform wiretap for law enforcement purpose. The first analog mobile phones provided No or very weak security which resulted in very serious embarrassment. In late 1980s, European GSM system designed provided better security but flaws remain .Most of these flaws addressed in 3GSM system but even end-to-end protection has not been provided. In next generation of smart phones user will install software with this capability, either directly for 3GPP voice stream or in VoIP protocol.This paper intend to give brief overview of the security approaches taken in selected No of protocol , focusing of wireless communication , general approach to security architecture .

II. GENERATION OF CELLULAR NETWORK

Cellular Network Started its beginning from 1980s when first generation (1G) network , introduced as first commercially automated analog based wireless telephone technology , mobile communication launched in Japan by NTT (Nippon Telegraph and Telephone) .cellular network . 1G Mobile phones had only voice facility which was replaced by second generation (2G) digital cellular telephony in 1991with added fax, data and messaging service s. The third generation (3G) launched in 2003 had advanced multimedia facilities to 2G phones with high speed digital cellular telephony (Including video telephony). And now talks on more advance technology 4G going to be launched soon. It’s a IP based “anytime, anywhere “voice, data, multimedia telephony at faster data rates than 3G.Cellular network / telephony is a radio based technology where base station transmits to and receive from mobiles at the assigned spectrum and service area of each station is called a cell .

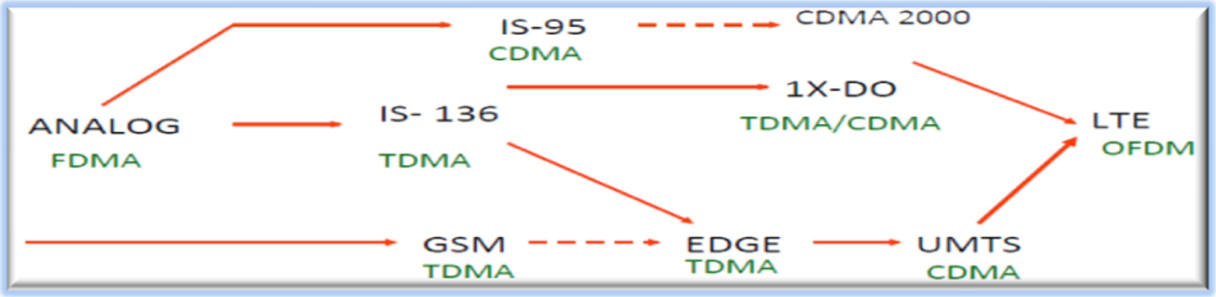


Fig: Evolution of Cellular Network

2.1.G &2.5G

2G Phones having using global system for mobile communication (GSM) were first used in early 1990s in Europe. GSM provides voice and limited data services and uses digital modulation for improved audio quality. 2G systems were significantly more efficient on the spectrum allowing for greater mobile penetration levels. All text messages sent over 2G are digitally encrypted , allowing for the transfer of data in such a way that only intended user can able to receive and read it .In addition to GSM Protocol , 2G also utilizes various other digital protocols , including CDMA,TDMA ,iDEN,& PDC . GSM is based on TDMA. 2.5G wireless technology is a stepping stone that bridged 2G to 3G wireless technology and used to describe those evolved technologies that were first considered as being 2G. While 2G and 3G were officially defined as wireless standards by the International Telecommunication Union (ITU), 2.5G was not defined as it was used only for the marketing purpose. However some of the data services which are the part of the 2.5G extensions are:

Short Messaging Service (SMS): Message transferred in one cellphone to others. Large message are truncated and sent as multiple messages.

High Speed Circuit: Switched Data (HSCSD): This was first attempt to provide data at high speed over GSM but was not widely implemented and GPRS become popular technique.

Cellular Digital Packet Data (CDPD): It is a packet based data service, able to detect idle voice channels and uses them to transfer data traffic without affecting voice communication.

2.2.G

3G is the third generation of the mobile phone standard and technology. It has been established through ITU's project on International Mobile Telecommunications 2000. In May 2001, NTT DoCoMo (Japan) launched the first pre-commercial 3G network – branded as FOMA. UMTS-HSPA is the world's leading 3G technology. By 2015, UMTS-HSPA and LTE 3G technologies are expected to account for 3.9 billion global subscriptions, compared to 569 million CDMA EV-DO subscription and 59 Million WiMAX subscription. A 3G technology based on Universal Terrestrial Radio Access (UTRA) radio interface and the extended GSM/GPRS network. A second radio interface also exists called IMT Multicarrier (IMT-MC) which is being promoted by the 3GPP2 organization. This interface is backward compatible with IS-95 to make a seamless transition to 3G. This process is commonly known as CDMA2000.

III. SURVIVABILITY CONCERN IN WIRELESS NETWORK

Network Survivability is an essential aspect of reliable communication services. It can be better describe in term of software engineering as capability of a system to fulfill its mission in a timely manner, even in the presence of attack and failures .It goes beyond Security and fault tolerance to focus on delivery of essential services, even when system are penetrated or experience failures and rapid recovery of full service when conditions improve. We can classify survivable mobile wireless networking requirements into four categories based on (i) Resistance requirement (ii) Recognition requirement (iii) Refinement requirement (iv) Recovery requirement.

Limitation of Cellular Network
System Complexity

Wireless system is more complex due to the need to support mobility and making use of the channel efficiently. By adding more complexity to the systems, potentially new security vulnerabilities can be introduced.

Limited Bandwidth

Although wireless bandwidth is increasing continuously due to channel contention everyone has to share the medium.

- **Congestion:** It occurs at a base station when it does not have enough space in its queues to put the new arriving packets. These new packet would then be lost .It lead to the packet already in queue to wait for the longest time before being transmitted due to which it leads to unacceptable packet delay.

- **Fading :**It occurs due to multipath and shielding. Multipath Fading is caused by the transmission of the signal along different paths and resulting in simultaneous reception .Depending of the amplitude d phase of signals due to which signals cancel each other completely or significant attenuation in the resultant signal. Shielding occur due to the absence of field strength due to tunnels, hills and inside certain building.

- **Co-Channel Interference :**Co-channel are the same channel that are used by different cells .To avoid this kind of interference, it is necessary to separate the co-channels as great distance as possible. This will lead to increase in channel capacity.

- **Relatively Unreliable Network Connection :** The wireless medium is an unreliable medium with a high rate of errors compared to wired network.

- **Infrastructure Needed :** Small cells require a complex infrastructure to connect all base station. The infrastructure required includes switches for call forwarding, location registers etc

Security Challenges in Cellular Network : A smartphone user is exposed to various threats when they use their phone. These threats can disrupt the operations of cell phones and transmit or modify any data. Thus application deployed there must guarantee privacy and integrity of the information they handle.

- **Authentication :** One way authentication based on long term shared key between user's SIM card and the home network .Each user has to be authenticated to ensure the right person are using the network . Issue of cross region and cross prodder authentication is an issue.

- **Privacy**
  - Data
    Link level encryption over the air but there is no protection over the core network.
  - Identity/Locations /Movements
    Uses of temporary identifiers reduce the ability of an eavesdropper to track movement within a specified region.

- **Web Service :** A web service is a used with functionality aspect using standard protocol which can results in major security incidents such as viruses,denial of service attacks etc .

- **Operating Systems in Cellphone devices :**Each phone varies with different software domain, some phone may use a Java based system other use Microsoft Window which can prove hindrance in OS which have open security hole.

- **Limit on Location Detection :** There should be the limit in tracking the actual location of phone through GPRS for Privacy concern. It should be made in law that only investigation agencies can trace the mobile location.

- **Contents which are downloaded :** Downloaded spyware can cause security threat. Unauthorized downloading of music, files etc can cause serious security threat in mobiles.

- **Device Security during Lost / Stolen :**If device is lost or stolen, then it needs to be protected from unauthorized use so that sensitive information like e-mails, phone numbers cannot be accessed.

Figure 1, shows threat model for a femto-cell-enabled mobile network . The three vulnerable elements are indicated by arrows (i) the air interface between mobile device and the femto-cell (ii) the femto-cell itself (iii)the public link between femto-cell and the security gateway . Intent is to focus on certain attacks which are achievable without breaking the protocols.

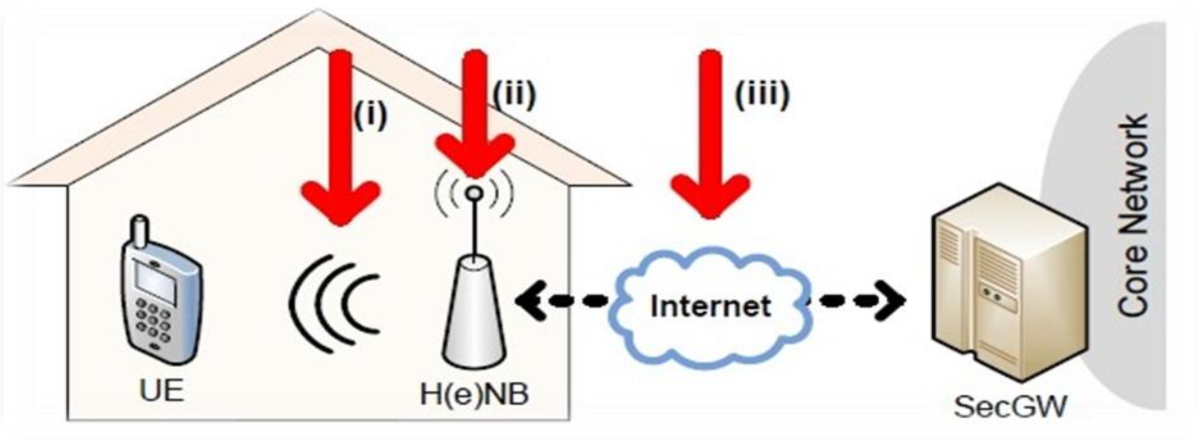


Fig 1 : Three different target for malicious attacks on femto-cell enabled mobile networks : (i)The air interface between the mobile device and the femto-cell (ii) the femto-cell itself (iii) the public link between the femto-cell and the security gateway .

- **Attacks on the Air Interface:** The attack on the air interface can be either passive or active .Although prerogatives for active attacks have been mitigated by cryptographically protecting the messages sent over the air , passive attacks , such as traffic analysis and user tracking are still possible .Subscriber identity and tracking are the emerging threats at the air interface in femto-cell enabled mobile networks .

- **Attacks on femto-cell :**A mobile device being connected to regular base station i.e., NodeB or a femtocell is both are same, because the protocols and the security standards used at the air interface .From a malicious user's part, it makes a substantial difference as it is much easier for a malicious user to tamper with a small and expensive femtocell than it could be with a large and complicated device located on a rooftop. The physical size and , material quality , lower cost components and the IP interface of the femtocell make it more suited for reverse engineering and tampering than a traditional , more expensive and business grade (e)NodeB base station . As the over air user data encryption is terminated at the femtocell , hardware tampering with the device could expose the private information of the unsuspecting user. Moreover , attacks such as device impersonation , Internet protocol attacks on the network services , false location reporting or unauthorized reconfiguration of the onboard radio equipment could hinder the network operator from controlling interface and power management features .This could leads to severe consequences on the quality of services . To this end ,femtocells should be equipped with execution environment that render malicious manipulation of the onboard software and the on-the-wire sniffing very hard to achieve .

Attacks on the Core Networks : The large scale deployment of less expensive upgrades to the back bone connection.But the exposure of the core network's point of entrance to the public Internet has severe drawbacks: Render most internet based attacks, such as Denial of service or impersonation attacks, feasible against the mobile network operator. The core networks are responsible for storage of subscriber information,billing, mobility management, authentication / authorization and routing of user data to hitsdestination. Without this infrastructure, the calls and data services cannot be successfully established. Usually, the core network is protected from external access by firewalls located at its edge. Inside the core network encryption is not specified for UMTS and not mandatory for LTE , although the IP interfaces in LTE can be protected by using IPSec secure connections among the RAN and CN components . As LTE supports interconnections with non – 3GPP networks such as WiMAXand WiFi ,IPSec tunnels are used inside the core network to protect the confidentiality of Information.

IV. TYPES OF ATTACK

Due to such a massive architecture of a cellular network, there are a variety of attacks that the infrastructure is open to:

- Denial Of Services (DOS)

This is one of the most potent threats that can bring down the entire network infrastructure. It is an attempt to make a machine or network resource unavailable to its intended users . It lead to the unusual slowness in network performance, disconnection of wireless or wired connection .Attacks can be fundamentally be classified into five families:

[1] Consumption of Computational resource such as bandwidth, memory, disk space.
[2] Disruption of state information, such as unsolicited resetting of TCP sessions.
[3] Disruption of physical network components.
[4] Obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately .
Disruption of configuration information such as routing information .

Distributed Denial of Services (DDoS) : A distributed denial of services attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming message to the target system forces it to shut down. In a type of DDoS attack malicious users first build a network of computers which they will use to produce the volume of traffic needed to deny services to computer users. To create this attack network, attackers discover vulnerable sites or host on the network. Vulnerable host are usually those that are either running no antivirus software or out of date antivirus software. The next step for the intruder is to install new programs on the compromised host of the attack network. The hosts that are running these attack tools are known as zombies and they can carry out any attack under the control of the attacker.

Attakers can use different kind of techniques in order to find vulnerable machines. The most important follow:

Random Scanning

In this technique, the machine that are infected by the malicious code probes IP addresses randomly from the IP address space and check their vulnerability .When it find any vulnerable machines or cellphones it break into it and tries to infect it by installing on some malicious code .Thistechnique create significant traffic as random scanning cause large number of compromised hosts to probe and check the same addresses.

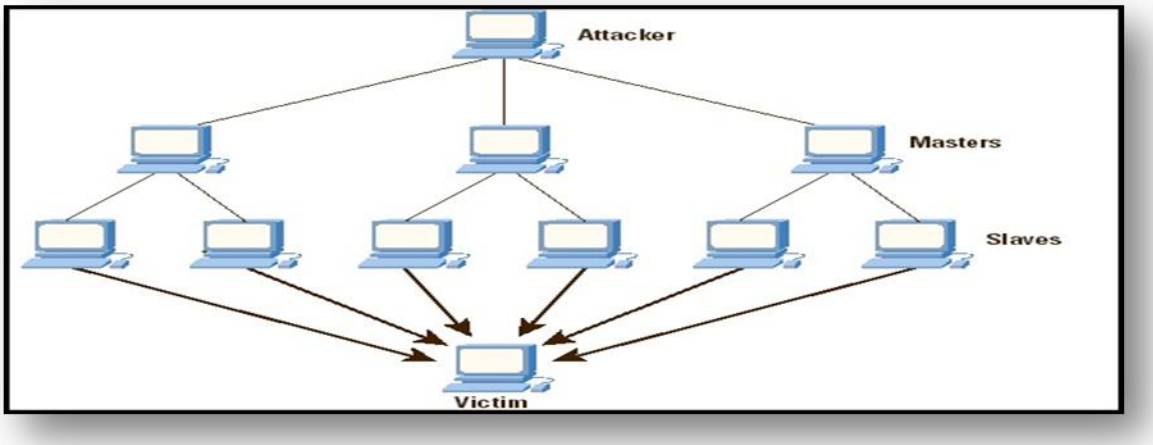


Fig : A DDoS Attack

Hit-List Scanning

Long before attackers start scanning they collect a list of large number of potentially vulnerable machines In their effort to create their army, they begin scanning down the list in order to find vulnerable machine When they find one, they install on it a malicious code and divide the list in half. Then they give one half to the newly compromised machine , keep the other half and continue scanning the remaining list The newly infected host begins scanning down its list , trying to find a vulnerable machine . When it find one , it implements the same procedure as describe above and in this way hit-list scanning take place simultaneously from an enduringly increasing number of compromised machines .

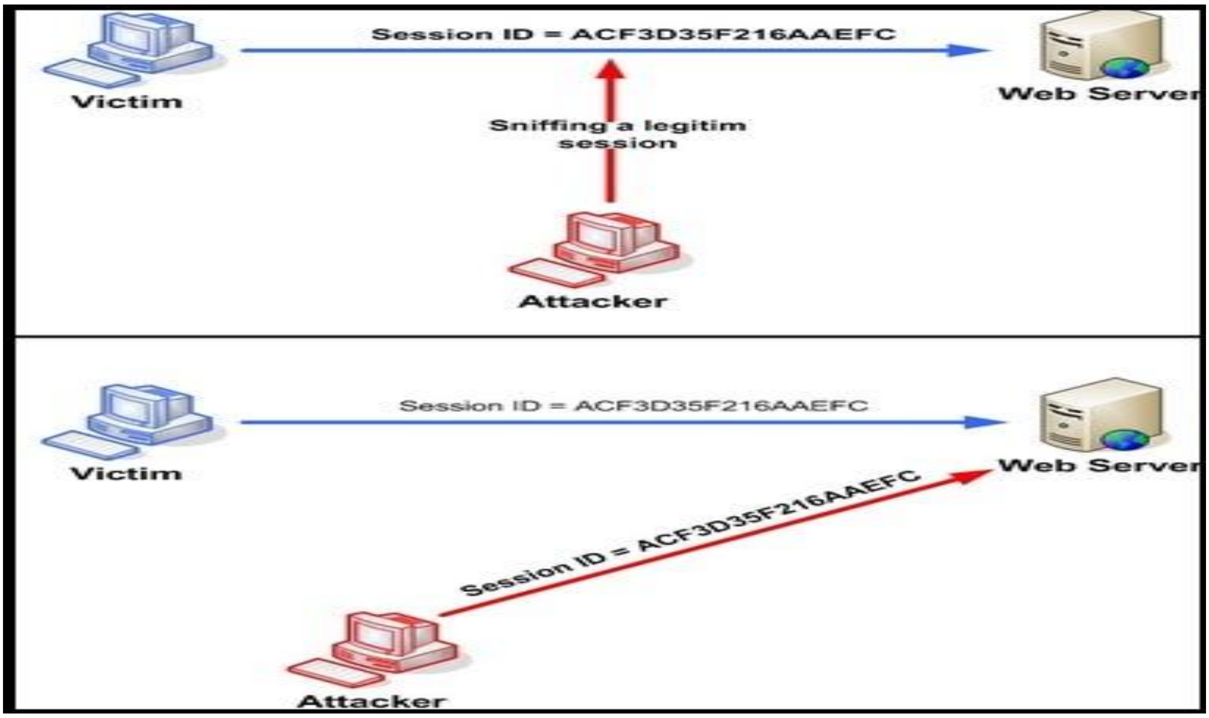
Topological Scanning

Topological scanning uses information contained on the victim machine in order to find out the new target .In this technique an already compromised host looks for URLs in the disk of a machine that it wants to infect .Then it renders these URL target and check their vulnerability. This scanning technique can create a large army of attackers extremely quickly and in that way can propagates the malicious code

Local Subnet Scanning
This type of scanning acts behind a firewall in an area that is considered to be infected by the malicious scanning program. The compromised host looks for targets in its own local network, using the information that is hidden in local addresses. In that way an army with numerous zombies can be constructed at an extremely high speed.

- **Session Hijacking**

It is also known as TCP session hijacking , a security attack on the user session over the protected network . This most common method of session hijacking is called IP spoofing, when an attacker's uses source routed IP packets to insert commands into an active communication between two nodes on a network and disguising itself as one of the authenticated users. This type of attack is possible as authentication typically is only done at at the start of the TCP Session.Eg : in the below diagram we can see first the attackers uses a sniffer to capture a valid token session called " Session ID " then he uses the valid token session to gain unauthorized access to the web server .


Session ID = ACF3D35F216AAEFC
Victim
Web Server
Sniffing a legitim session
Attacker
Session ID = ACF3D35F216AAEFC
Victim
Web Server
Session ID = ACF3D35F216AAEFC
Attacker

- **Message Replay :** A message replay attack is one in which an attacker eavesdrops, obtains a copy of an encrypted message and then re-uses the message at a later time in an attempt to trick the cryptographic protocol. In order to control the replay detection on the client using code creates a **SecurityBindingElement** to use in a **Custom Binding**.

- **Eavesdropping :**It is an un-authorized real time interception of a private communication such as phone calls, private message etc. It is easier to perform with IP based calls than TDM based calls .Any protocol analyzer can pick and record the call without being observed by the callers.

- **Message forgery :**It is the sending of a message to deceive the recipient as to whom the real sender is. A common example is sending a spam file as if it were originated from an address other than the one which was really used. Attacker can change the content without the user ever knowing.

3G Security Architecture

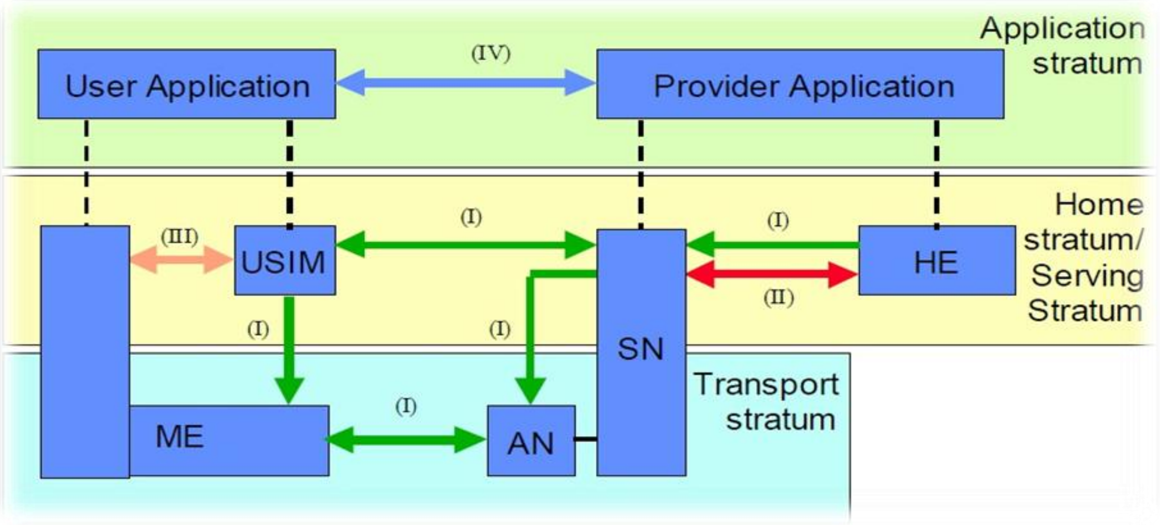


Fig: Overview of the Security Architecture

There are five security feature groups which meet certain threats and accomplish certain security objectives.

- Network Access Security (I)
  It's a set of security features that provide users with secure access to 3G services and which in particular protect against attacks on the radio access link.
- Network domain security (II)
  It's a set of security features that enables nodes in the provider domain to securely exchange signaling data and protect against attacks on the wire line network.
- User domain Security (III)
  The set of security features that secure access to the mobile stations.
- Application domain Security (IV)
  The set of security features that enables applications in the user and in the provider domain to securely exchange messages.
- Visibility and configurability of security (V)
  The set of features that enables the user to inform himself whether a security features is in operation or not and whether the use and provision of services should depend on the security features.

The UMTS connection setup consists of three stages including the identification, AKA and security mode setup. At the identification stage , MS sends its identity to VLR /SGSN via SRNC . The Purpose of UMTS AKA is to set up a mutual authentication as well as established a pair of cipher and integrity keys between VLR/SGSN and USIM (I) . The entries MS, VLR/SGSN and HLR /AuC (HE) are involved in UMTS AKA Protocol .At the security mode setup stage , MS responses to the command of VLR/SGSN which is about the preferred ciphering and integrity check algorithms.The UMTS AKA Process utilizes the secret key (K) and the cryptographic algorithm including f1,f1*,f2,f3,f4,f5 and f5* shared between the MS and HE. Also in order to check the freshness of the received message and prevent the replay attack , HE and MS uses the counter (SQNhe) and (SQNms) respectively .These counters produce the two sequence of numbers which will be compared with each other in time of protocol execution . The authentication protocol is based on secret key K, which is unique for each user and resides only in USIM and the database in HE. As per illustrated in below figure the UMTS identification, distribution of authentication data, AKA, and security mode setup protocol work as follows

Identification

The MS sends the security capabilities including UIA (UMTA integrating Algorithm) and UEA (UMTS Encryption Algorithm) with START value of CS service domain to SRNC . Also the MS transfers the initial L3 message including its IMSI to VLR/SGSN via SRNC . By this message the MS request for services like location update , CM (Connection management) service , routing area update.

Distribution of authentication data

The VLR / SGSN identifies the MS by its IMSI and then send the authentication data request including the MS 's IMSI and the requesting node type (PS or CS) to the HE . Then HE sends an authentication data response back to VLR/SGSN that contained an array of n authentication vectors AV (1…n). The generation of AV , which includes RAND , XRES , CK, IK and AUTN in shown in fig below

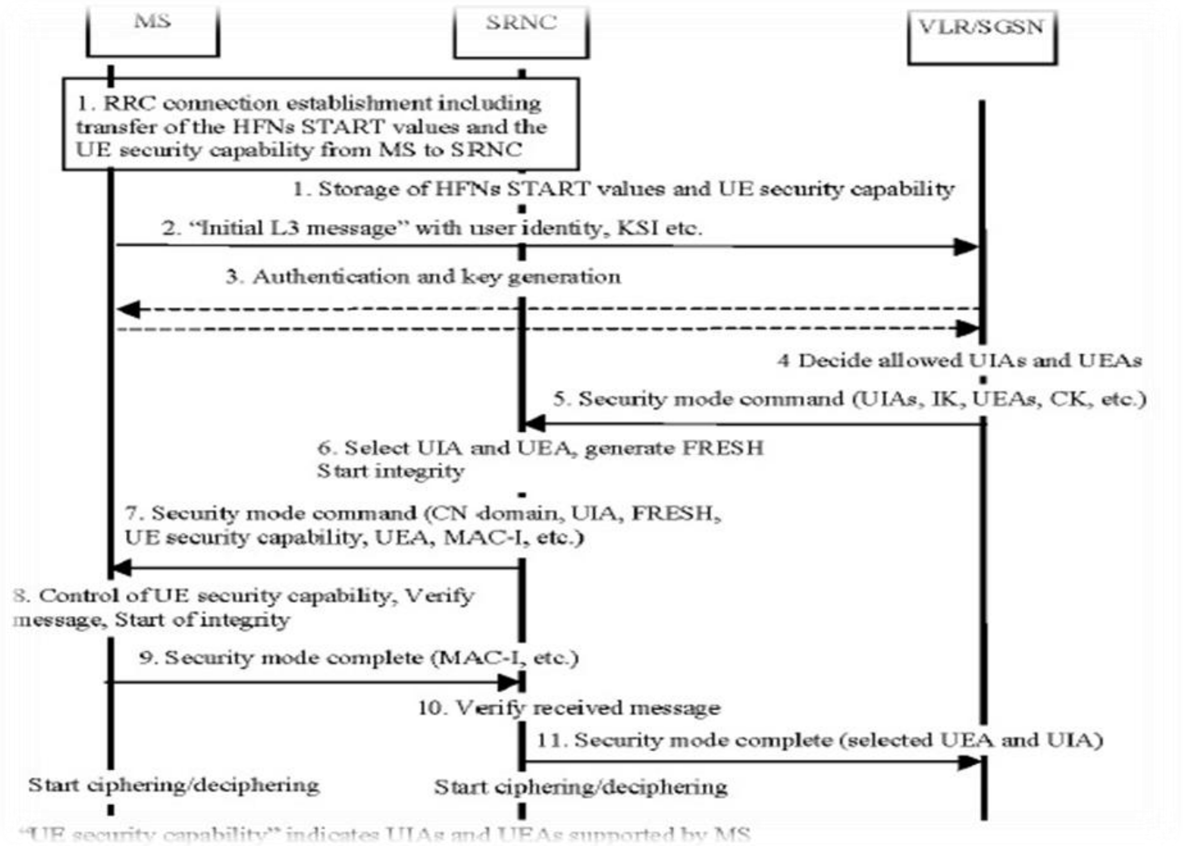

MS
SRNC
VLR/SGSN
1. RRC connection establishment including transfer of the HFNs START values and the UE security capability from MS to SRNC
1. Storage of HFNs START values and UE security capability
2. "Initial L3 message" with user identity, KSI etc.
3. Authentication and key generation
4 Decide allowed UIAs and UEAs
5. Security mode command (UIAs, IK, UEAs, CK, etc.)
6. Select UIA and UEA, generate FRESH Start integrity
7. Security mode command (CN domain, UIA, FRESH, UE security capability, UEA, MAC-I, etc.)
8. Control of UE security capability, Verify message, Start of integrity
9. Security mode complete (MAC-I, etc.)
10. Verify received message
11. Security mode complete (selected UEA and UIA)
Start ciphering/deciphering
Start ciphering/deciphering
"UE security capability" indicates UIAs and UEAs supported by MS

Fig : The UMTS identification , distribution of authentication data , AKA , and security mode setup Procedure (I)

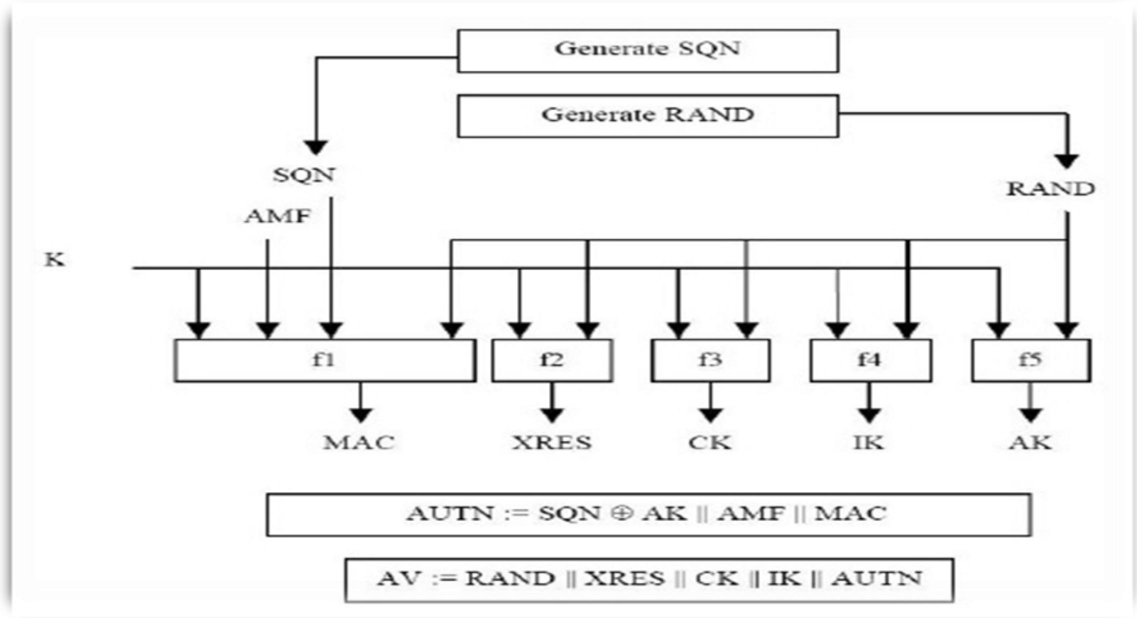

Generate SQN
Generate RAND
SQN
RAND
AMF
K
f1
f2
f3
f4
f5
MAC
XRES
CK
IK
AK
AUTN := SQN ⊕ AK || AMF || MAC
AV := RAND || XRES || CK || IK || AUTN

Fig : Generation of Authentication Vectors

Authentication and key management

The VLR / SGSN chooses the next unused AV from the ordered array of AVs in the VLR /SGSN database on the basis first -in / first -out . Then the VLR / SGSN sends to the MS a random challenge (RAND) and an authentication token (AUTN) from the chosen AV.The operation of MS upon the receipt of RAND || AUTN is illustrated below . The MS first computes the anonymity key AK= f5k(RAND) and retrieves the sequence number . Then the MS computes XMAC=f1k(SQN||RAND||AMF) and compare it with MAC included in AUTN . If they are same then MS verifies if the SQN is in correct range compared to its sequence number . The VLR /SGSN compares the received RES with XRES . If they are equal , the AKA process of the MS is successfully completed .

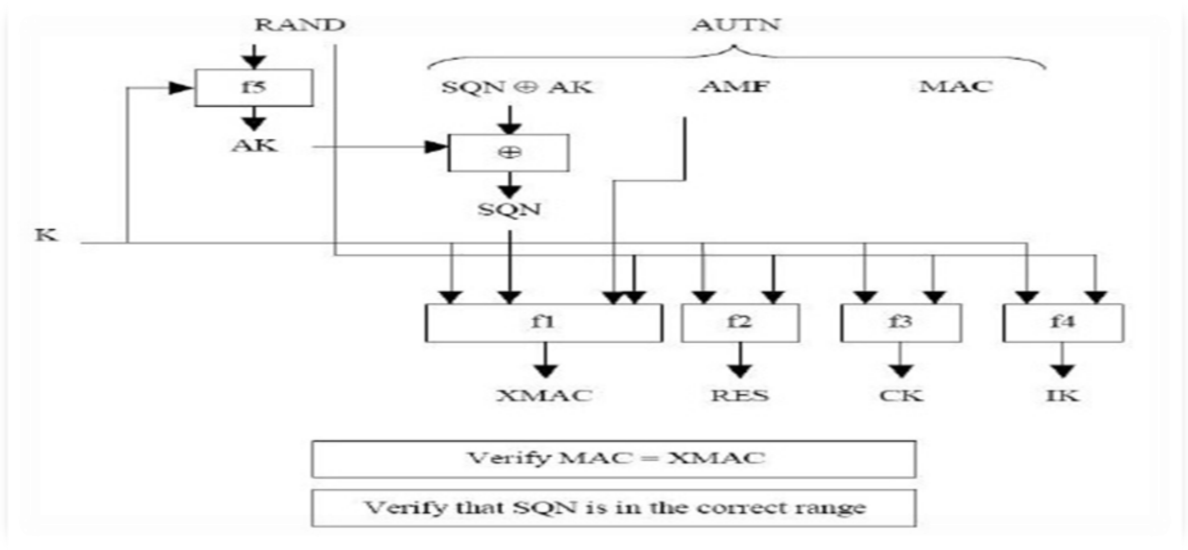


Fig : User Authentication Function in MS

Wireless Application Protocol

Wireless Application protocol (WAP) is an application environment and set of communication protocol for wireless device designed to enable manufacturer vendor and technology independent access to the internet and advance telephony services.WAP utilizes Internet standard such as XML user datagram protocol (UDP) and Internet Protocol (IP). WAP utilizes binary transmission for greater compression of data and is optimized for long latency and low bandwidth. WAP session cope with intermittent coverage and can operate over a wide variety of wireless transport.

Architecture of WAP gateway

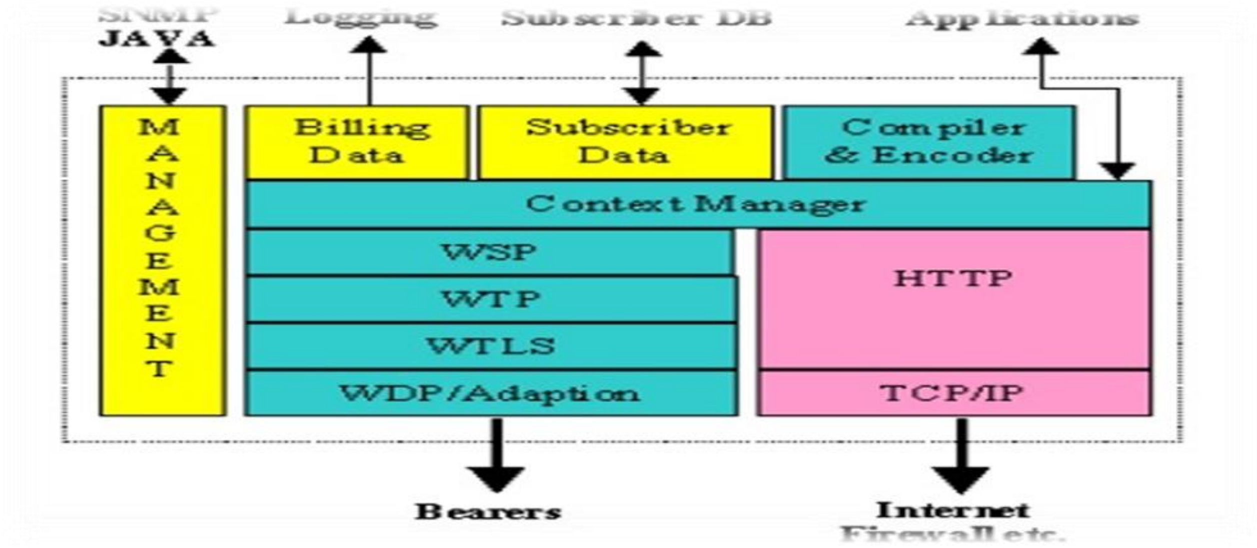


Fig : Architectural View of WAP gateway

WDP : The WAP diagram protocol (WDP) is the transport layer that sends and receives messages via any available bearer network including SMS , USSD,CSD,CDPD, IS-136 packet data and GPRS .

WTLS: Wireless transport layer security , an optional security layer has encryption facilities that provide the secure transport service required by many application . The WAP transaction protocol (WTP) layer provides transaction support , adding reliability to the datagram service provided by WDP.

WSP : The WAP session protocol (WSP) layers provides a light weight session layer to allow efficient exchange of data between applications.

HTTP Interface : It Serve to retrieve WAP content from the Internet requested by the mobile device . WAP content (WML and WML Script) is converted into a compact binary form from transmission over the air .

Future : Security in Wireless Cellular will remain in year around and there will be malicious users trying to exploit the security breach in mobile network. Thus time is to concentrate on more developed network architecture for wireless cellphones as mobile device revolution is quite possible to most significant change in computing since we shifted from the main frame more than 20 years ago. These handheld device features ubiquitous , connectivity ,constant access to the biggest repository of mankind's knowledge and more computing power than the NASA control room for the first moon landing .

A Look at Security in 4G : Future 4G mobile communication networks are expected to provide allIP-*based*services forheterogeneous wireless access technologies assisted by mobile IP to provide seamless Internet access for mobile users. 4G support for interactive multi-media services like video teleconferencing etc , scalability of mobile networks and higher bandwidth up-to 100Mbps .Two major challenges in developing such heterogeneous network infrastructure are QoS provisioning and security services for mobile user communication flow. The Primary weakness in 4G security is that its use of cryptography does not provide end-to-end security. It only encrypts the traffic between the phone and the base station but there is no encryption while the data is communicated over wired network. It means there is no security against malicious or compromised carrier.

Summary : Mobile and wireless security need to be addressed by both the users of technology and law enforcement agencies in order to minimize the risk of criminal misuse. In addition while issues related to authenticated encryption , mutual entity authentication and access control are now well understood , most solution still have problems related to password guessing , privacy and denial of service . Surprisingly, 30 years after its invention public key cryptography is not widely deployed at lower layer in wireless environment. It is expected that in next decade the cost and usability of public key technologies will be reduced, which will deploy more advanced solution offering better privacy and robustness.In this paper we have reviewed some significant threats to security and privacy in femtocell- enabled mobile networks and has presented solutions direction to mitigate two among the most relevant and immediate ones First we discussed the issues related to the identity and location tracking with femtocell technology. Second we discussed on survivable networks requires more than conventional reliability and fault tolerance .Survivable mobile wireless network require that asymmetric , weekly connected and episodically disconnected links be considered as first class citizen rather than faults that must be occasionally repaired .

V. ACKNOWLEDGEMENT

Presenting this research paper was great challenge for me , but I duly express my gratitude to my guide , mentor & curator **Dr R. P Mahapatra** , HOD(Computer Science Engineering) , SRM University , Ghaziabad , who helps me in every time with his innovative points ,explanation of my doubts & constant inspiration.I duly express my gratitude to my almighty GOD & my parents without their blessing & grace it was not possible to complete this innovative paper.

REFERENCE

[1] 3GPP TS 33.102 V8.0.0 (2008-06), 3GPP Technical Specification Group Services and System Aspects, 3G Security, Security Architecture (Release 8).

[2] William Stallings, Cryptography and Network Security: Principles and Practice, Prentice-Hall, July 1998, ISBN 0138690170.

[3] National Institute of Standards and Technology (NIST), Advanced Encryption Standard (AES), Federal Information Processing Standards Publications (FIPS PUBS) 197 (2001).

[4] H. Dobbertin, L. Knudsen, and M. Robshaw, "The cryptanalysis of the AES - a brief survey", Advanced Encryption Standard C AES: 4th International Conference, AES 2004, volume 3373 of Lecture Notes in Computer Science, pp. 1–10, Springer-Verlag, 2005.

[5] C. E. Shannon, "A Mathematical Theory of Communication", the Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656, July, October, 1948.

[6] W.S. Juang and J.L. Wu, "Efficient 3GPP Authentication and Key Agreement with Robust User Privacy Protection", IEEE Communications Society, Proceedings of the WCNC, 2007.

[7] [Fernandez05-1] Fernandez, E., et. al., "An overview of the security of wireless networks," Handbook of Wireless

[8] Afek Y., and E. Gafni, "End-to-End Communication inUnreliable Networks," Proc. Seventh Annual ACM Symp. Onthe Principles of Distributed Computing, Toronto, Ontario,Canada, 1988, pp. 131–148.

[9] Lauter, K., "The Advantages Of Elliptic Curve Cryptography For Wireless Security," Wireless Communications, IEEE Feb 2004 Volume: 11, Issue: 1 On page(s): 62- 67

[10] "Channel Surfing and Spatial Retreats: Defenses against Wireless Denial Of Service,"Proceedings of the 2004 ACM workshop on Wireless security, 2004

[11] **http://www.winlab.rutgers.edu/~trappe/Papers/WiDoS_Wise04.pdf**

List of Acronyms

[1] 1G - First Generation Cellular Networks
[2] 2G - Second Generation Cellular Networks
[3] 3G - Third Generation Cellular Networks
[4] 3GPP - 3rd Generation Partnership Project
[5] 4G - Fourth Generation
[6] AMPS - Advanced Mobile Phone System
[7] CDMA - Code Division Multiple Access
[8] CDPD - Cellular Digital Packet Data
[9] D-AMPS - Digital AMPS
[10] EDGE - Enhanced Data Rate for GSM Evolution
[11] GGSN - Gateway GPRS support node
[12] GPRS - General packet Radio Service
[13] GSM - Global System for mobile communication
[14] HSCSD - High Speed circuit switched Data
[15] IMT - International Mobile Telecommunications
[16] ITU - International Telecommunication Union
[17] NA-TDMA - North American Time Division Multiple Access
[18] NMT - Nordic Mobile Telephony
[19] PCS - Personal communication services