A Survey on Wireless Security

Surjit Paul[1], Sanjay Kumar[2]

[1]M.Tech CSE Scholar, Dept. of Computer Science and Engineering, NIT Jamshedpur, Jharkhand, India
[2]Associate Professor, Dept. of Computer Science and Engineering, NIT Jamshedpur, Jharkhand, India

Abstract- *A Wireless Network is a wireless communication system that allows mobile computers and workstations to communicate and exchange data with each other using radio waves as the transmission medium. Nowadays wireless networks are used in many areas such as universities, healthcare-centers, hospitals, police department, military, airports, etc. WLAN (Wireless LAN) is commonly referred to as "Wi-Fi" (wireless fidelity) that gives freedom to move mobile nodes like laptops, PDA, etc. from one place to another within their offices and organizations without the need of wires and without losing network connectivity. Most of the businesses, research, day to day activity, etc. are shifting from wired to wireless. At present the wireless system is not very secured and needs various hardware and software techniques to protect the data/information from unauthorized access. Therefore, it is essential to enhance the network security in order to protect the information in the wireless network. This survey paper deals with various security protocol standards, attacks, threats, etc. in WPAN, WMAN and WWAN.*

Keyword: - **PDA, Threats, Attacks, WPAN, WMAN, WWAN**

1. INTRODUCTION

Wireless networks becoming more and more popular now a days. People from all spheres of the globe are either shifted or intend to shift from wired to wireless due to the availability of various features of wireless technology. In present scenario, the popularity of wireless networks has potential towards the fulfillment of their requirements, such as: user mobility, fast and simple installation, flexibility, scalability and relatively low price. WPAN (Wireless Personal area Networking) is a mobile adhoc network formed by mobile devices connected by Bluetooth. This is a small network called as piconet. It supports a short range wireless communication. WLAN (Wireless Local Area Network) enables users to access resources no matter of their location within the wireless network. In WMAN (Wireless Metropolitan Area Networking) internet is used as the backbone and different access points help mobile devices to communicate with each other. In WWAN (Wireless Wide Area Network) different technologies are used like CDMA, GSM, 3G, 4G/LTE and LTE advance. Data are transferred via radio waves spreading throughout the space and thus the information reaches anyone with the appropriate radio receiver. Therefore, there is a problem of the protection of information. Traditional mechanisms for the physical protection of wired networks (firewalls and shields) cannot be applied to the protection of wireless networks. It was necessary to create mechanisms for the protection of the wireless networks in order to enable users to use wireless networks and feel sure about the accuracy of information and their privacy. Initialization key, unit key, combination key and master keys are used in WPAN. 802.11i standard for wireless local networks introduces WEP (Wired equivalent privacy) protocol to solve the problems of protection similar to the protection level of wired local networks. Privacy Key Management (PKM) protocol uses X.509 certificate issued by manufacturers in WMAN. GSM uses A3, A8 and A5 algorithms for protection in WWAN. The rest of the paper is organized as follows; Section 2 specifies security issues in wireless networks, Section 3 deals with various kinds of attacks in wireless network. Section 4 deals with the basic security issues in WPAN. Section 5 deals with security issues in WMAN (WiMax) and Section 6 deals with security issues in wireless wide area network (WWAN) and its futuristic technologies and finally section 7 deals with conclusion and future work.

2. SECURITY ISSUES IN WIRELESS NETWORKS

2.1 Security Issues

Integrity, confidentiality, nonrepudiation and availability are the key issues related to security in the wired as well as in wireless network.

Integrity: Integrity can refer to either system integrity or data integrity. A system provides integrity if it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. Data integrity is maintained, if the receiver of the data can verify that the data have not been modified and does not contain fake data.

Confidentiality: It refers that only intended recipient can read the authorized data because of access mechanism protections, or other means, such as encryption. It further protects the data even if they are stolen or intercepted.

Nonrepudiation: The Security issue in which the sender should not be able to falsely denying of sending the data. In electronic commerce, vendors do not want their clients to deny that they made purchases and thus must pay for any services or goods they received.

Availability: The property of the systems in which a third party with no access authorization should be able to block legitimate parties from using a resource. Using Denial-of-service (DoS) attack, attacker can involve one site flooding with traffic or one site sending a small stream of packets designed to exploit flaws in the operating system's software that take the site down.

3. VARIOUS KINDS OF ATTACKS IN WIRELESS NETWORK

Traffic analysis: It is a very simple technique that enables an attacker to take over a packet during its transmission. This technique enables the attacker to have access to three types of information i.e. identification of activities on the network, the identification and physical location of AP (Access Point) in its surroundings and getting information about the communication protocol by traffic analysis. An attacker needs to gather the information about the size and number of the packet over a certain period of time.

Passive eavesdropping: This technique is used to watch over an unlimited wireless session. The only condition to be fulfilled is that the attacker has the access to the area of emission. With a decrypted session, the attacker is able to read the data during its transmission and gather them indirectly by surveying the packets. This kind of attack is not based on violation of privacy, but information gathered in this way can be used for more dangerous kinds of attacks. **Active eavesdropping:** During this type of attack, the attacker watches over a wireless session and actively injects his own messages in order to reveal the content of the messages in the session. Precondition for this type of attack is to access the communication area and some knowledge on the part of the message, such as IP address. The attacker is able to modify the content of the packet so that the integrity of the message remains preserved. Usually the attacker changes final IP or TCP address. The attacker injects messages known only to him into the traffic in order to create conditions for decryption of the packets that should be received by other wireless users. These conditions are created by creating IV (Initialization Vector) sequence and message for each single message that is sent. After some time, when a packet with the same IV as in the database appears, the attacker is able to decrypt the message. The only way to prevent this kind of attacks is to change WEP key often enough.

There are three techniques that can violate the integrity of the traffic i.e. unauthorized access, hijacking attack and replay attack [1]. In order to successfully implement these techniques, it is necessary to apply attack techniques for privacy and unauthorized access. The above mentioned attacks are directed towards the network in general, not towards users. But, once the attacker gets access to the network, he is able to initiate some other types of attacks or use network without being noticed. Some may think that unauthorized use of the network is not a significant threat to the network since the access rights allocated to resources will disable the attackers. However, usually an unauthorized access is the key to initialization of ARP (Address Resolution Protocol) attacks. VPN (Virtual Private Network) and IPsec solution can protect users from the attacks that directly influence the confidentiality of application data, but it cannot prevent attacks that indirectly ruin confidentiality. The Man in the middle, hijacking and replay attacks are the best examples of these kinds of attacks.

Man-in-the-middle-attack: This attack enables data reading from the session or modifications of the packet which violate the integrity of the session. There are several ways to implement this type of attack. One is when an attacker disrupts the session and does not allow the station to reestablish communications with the AP. The station tries to establish a session with the wireless network through AP, but can do that only through the workstation of the attacker pretending to be AP. At the same time, the attacker establishes connection and authentication with the AP. Now there are two encrypted tunnels instead of one: one is established between the attacker and AP, while the second is established between the attacker and the station. This enables the attacker to get access to the data exchanged between the workstation and the rest of the network.

ARP attacks: This is the sub-type of the man in-the-middle attack since these attacks are directed towards one component to wired network [2] and towards wireless clients [3]. The attacker escapes authentication or provides false accreditations. By getting the false accreditations, the attacker becomes a valid user and gets the access to the network as an authenticated user.

Hijacking attacks: In this type of attack, the attacker deprives the real owner of the authorized and authenticated session. The owner knows that he has no access to the session any more, but is not aware that the attacker has taken over his session and believes that he has lost the session due to ordinary failures in network functioning. Once the attacker takes over a valid session, he can use it for various purposes over a certain period of time. Such an attack could be combined with DoS attack [4]. It happens in a real time.

Replay attacks: This type of attack is used to access the network through authorization. The session under attack does not change or disrupt in anyway. The attack does not happen in a real time. The attacker gets the access to the network after the original session expires. He comes to the authentication of one or more sessions, and then replies to the session after a certain period of time or uses a couple of sessions to compose the authentication and reply to it. There are several types of DoS (Denial of Service) attacks that can violate availability of the network. Jamming and attack on 4-way handshake are only some of the DoS attacks.

Jamming: Jamming [5,6] is one of DoS attacks on network availability. It is performed by malicious attackers who use other wireless devices to disable the communication between users in a legitimate wireless network.

Attack on 4-way handshake: The last phase in the authentication process i.e 4-way handshake process, proved to be unsafe for DoS attacks. Though some of the attacks start in the first phase of the authentication process, but appear during the 4-way handshake process. In order to prevent the processor and the waste of memory resources, static and dynamic 4-way handshake solutions for protection from DoS attacks [7], as well as solutions for early detection of DoS attacks in the first phase of the authentication [8] have been introduced.

4. BASIC SECURITY ISSUES IN PERSONAL AREA NETWORK (PAN)

Wireless personal area networks (WPANs) provide connectivity among nodes relatively closer to each other within 10 meters range. Bluetooth is an industry standard protocol for WPANs and now it is developed as one of IEEE 802 standards i.e. 802.15. Bluetooth is also called wireless cable that connects different devices.

- **Ad Hoc Networks of Multiple Types of Devices:** PDAs, Laptops, Mobile Phones etc.
- **Piconets:** Small Clusters (Max Size 8) of Devices Forming an Ad Hoc Network. Masters Determine the Frequency. Piconet Example: Transfer of Files between Participants at a Meeting.
- **Scatternets:** Larger Networks Formed of up to 10 piconets.

Three classes of Bluetooth transmission are:

Class1: 100 mW max 100 metres range

Class2: 2.5 mW upto 50 metres range

Class3: 1 mW max 10 metres range

Bluetooth supports point-to-point (unicast) and point-to-multipoint (multicast) transmission with a variety of data rates.

Bluetooth Security Modes: Bluetooth defines three modes of security for devices: nonsecure, service level enforced security and link-level enforced security.

a) **Nonsecure:** A device is in nonsecure mode does not provide any security procedure. This is intended for public use devices, such as a wireless printer.
b) **Service-level enforced security:** A device in the service-level enforced security mode permits access to itself depending on the service request.

c) **Link-level enforced security:** A device in the link-level enforced security mode requires authentication and authorization for use, e.g. cell phones.

The Bluetooth standard defines security levels for devices and services.

Security levels for devices:

1. Trusted
2. Untrusted

Security levels for services:

1. Open
2. Authentication
3. Authentication and Authorization

Bluetooth Security Mechanisms: Bluetooth uses encryption and link-layer keys. Encryption keys protect the data in a session, whereas link-layer keys provide authentication and serves as a parameter when deriving the encryption keys. Link-layer key can be used after the current session to authenticate Bluetooth devices.

The four basic types of link-layer keys used in Bluetooth security are

- Initialization key
- Unit Key
- Combination Key
- Master Key

Initialization key: The security layer uses the initialization key of form a secure channel to exchange other link-layer keys. It creates the initialization key by using a combination of a PIN (Personal Identification No.) code. E22 algorithm is used to make an initialization key.

E22 (PIN (1-16 bytes), Bluetooth_Device_Address (6 bytes), Random No. (16 bytes))

Unit Key: It is generated in installation of a device, stored in nonvolatile memory. Unit and combo keys generated with the same function, different inputs.

E21 (Bluetooth_Device_Address (16 bytes), Random No. (16 bytes))

Combination key: The combination key is generated during the initialization process if the devices have decided to use one. It is generated by both devices at the same time. First, both of the units generate a random number. With the key generating algorithm E21, both devices generate a key, combining the random number and their Bluetooth device addresses. After that, the devices exchange securely their random numbers and calculate the combination key to be used between them.

Master key: The master key is the only temporary key of the link keys described above. It is generated by the master device by using the key generating algorithm E22 with two 128-bit random numbers. As the entire link keys are 128 bits in length, the output of the E22 algorithm is 128 bits, too. The reason for using the key generating algorithm in the first place is just to make sure the resulting random number is random enough. A third random number is then transmitted to the slave and with the key generating algorithm and the current link key an overlay is computed by both the master and the slave. The new link key (the master key) is then sent to the slave, bitwise XORed with the overlay. With this, the slave can calculate the master key. This procedure must be performed with each slave the master wants to use the master key.

Encryption: The Bluetooth encryption system encrypts the payloads of the packets. This is done with a stream cipher E0, which is re-synchronized for every payload. The E0 stream cipher consists of the payload key generator, the key stream generator and the encryption/decryption part. You can find a detailed C implementation of the E0 stream cipher in. The payload key generator combines the input bits in an appropriate order and shifts them to the four Linear Feedback Shift Registers (LSFR) of the key stream generator. The key stream bits are generated by a method derived from the summation stream cipher generator by Massey and Rueppel. Depending on whether a device uses a semi-permanent link key or a master key, there are several encryption modes available. If a unit key or a combination key is used, broadcast traffic is not encrypted. Individually addressed traffic can be either encrypted or not. If a master key is used, there are three possible modes. In encryption mode 1, nothing is encrypted. In encryption mode 2, broadcast traffic is not encrypted, but the individually addressed traffic is encrypted with the master key. And in encryption mode 3, all traffic is encrypted with the master key. As the encryption key size varies from 8 bits to 128 bits, the size of the encryption key used between two devices must be negotiated. In each device, there is a parameter defining the maximum allowed key length. In the key size negotiation, the master sends its suggestion for the encryption key size to the slave. The slave can either accept and acknowledge it, or send another suggestion. This is continued, until a consensus is reached or one of the devices aborts the negotiation. The abortion of the negotiation is done by the used application. In every application, there is defined a minimum acceptable key size, and if the requirement is not met by either of the participants, the application aborts the negotiation and the encryption cannot be used. This is necessary to avoid the situation where a malicious device forces the encryption to be low in order to do some harm. The encryption algorithm uses four LFSRs of lengths 25, 31, 33 and 39, with the total length of 128. The initial 128-bit value of the four LFSRs is derived from the key stream generator itself using the encryption key, a 128-bit random number, the Bluetooth device address of the device and the 26-bit value of the master clock. The feedback polynomials used by the LFSRs are all primitive, with the Hamming weight of 5. The polynomials used are (25, 20, 12, 8, 0), (31, 24, 16, 12, 0), (33, 28, 24, 4, 0) and (39, 36, 28, 4, 0). Information on the fundamentals of LFSRs is found in.

Authentication: The Bluetooth authentication scheme uses a challenge-response strategy, where a 2-move protocol is used to check whether the other party knows the secret key. The protocol uses symmetric keys, so a successful authentication is based on the fact that both participants share the same key. As a side product, the Authenticated Ciphering Offset (ACO) is computed and stored in both devices and is used for cipher key generation later on.

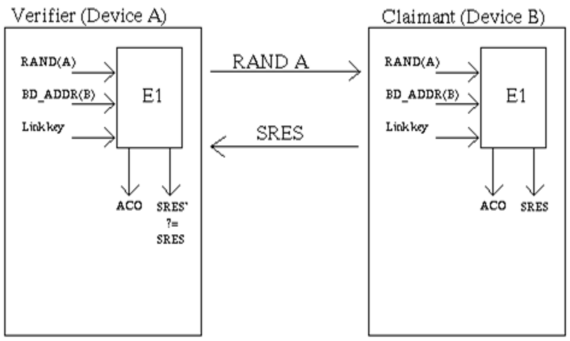

Fig -1: Authentication Process

5. Security Issues of WMAN (WiMax)

IEEE 802.16 protocol is the latest standard for wireless networks. It was established in 1999 to prepare specifications for broadband wireless metropolitan area networks. The first 802.16 standard was approved in December 2001 and was followed by three amendments: 802.16a, 802.16b and 802.16c. In 2004 the 802.16-2004 standard (IEEE-SA, 2006) was released and the earlier 802.16 documents including the a/b/c amendments were withdrawn. An amendment to 802.16-2004, IEEE 802.16e-2005 (formerly known as IEEE 802.16e), addressing mobility, was concluded in 2005. This implemented a number of enhancements to 802.16-2004, including better support for Quality of Service, Security and the use of Scalable OFDMA, and is sometimes called “Mobile WiMAX”, after the WIMAX forum. Currently active WiMAX amendments are: 802.16e- 2005- Mobile 802.16; 802.16f-2005- Management Information Base; 802.16g-2007-Management Plane Procedures and Services; 802.16k-2007-Bridging of 802.16 (an amendment to 802.1D). There are several amendments under development: 802.16h-Improved Coexistence Mechanisms for License-Exempt Operation; 802.16i- Mobile Management Information Base; 802.16jMultihop Relay Specification; 802.16Rev2-Consolidate 802.16-2004, 802.16e, 802.16f, 802.16g and possibly 802.16i into a new document. IEEE 802.16 Task Group m (TGm) is working on new amendment: 802.16mAdvanced Air Interface. The Proposed work plan would allow completion of the standard by December 2009 for approval by March 2010. In the IEEE 802.11 technology, security was added later. In IEEE 802.16, security has been considered as the main issue during the design of the protocol. However, the security mechanism of the IEEE 802.16 (WiMAX) still remains a question. WiMAX is relatively a new technology; not deployed widely to justify the evidence of threats, risk and vulnerability in real situations. Security within the MAC layer is called the security sublayer. Its goal is to provide access control and confidentiality of the data link. The separate security sublayer provides authentication, secure key exchange, and encryption. EAP Method, EAP encapsulation/ decapsulation RSA-based authentication/ SA control PKM control management Traffic data encryption / authentication processing Control message processing Message authentication processing PHY SAP Scope of IEEE 802.16 Specification Scope of recommendation (Out of Scope).

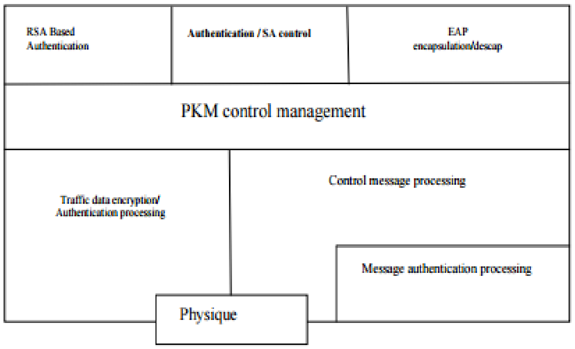
RSA Based Authentication
Authentication / SA control
EAP encapsulation/descap
PKM control management
Traffic data encryption/ Authentication processing
Control message processing
Message authentication processing
Physique

Fig -2 IEEE 802.16 security sublayer

When two parties establish a link, they are protected via a set of protocols that ensure confidentiality and unique access of the authorized parties. The unique handshaking between the two entities; namely base station (BS) and subscriber station (SS), is done at the MAC layer through security sublayer, which is based on the following concepts [2]: Security associations: A security association (SA) is a set of security information parameters that a BS and one or more of its client SSs share in order to support secure communications. Data SA has a 16 bit SA identifier, a Cipher (DES in CBC mode) to protect the data during transmission over the channel and two traffic encryption keys (TEKs) to encrypt data: one is the current operational key and the other is TEK [3]. When the current key expires, TEK a 2bit key identifiers is used. A 64bit IEEE 802.16 Security Issues.

There are Three types of SAs are defined [4,5]: primary, static, and dynamic. Each manageable SS establishes a Primary Security association during the initialization process. Static SAs are provisioned within the BS. Dynamic SAs are used for transport connections when needed. Both Static and Dynamic can be shared by multiple SSs. It may use separate SAs for uplink and downlink channels [6]. BS ensures that each SS has access only to its authorized SAs.

Public key infrastructure (PKI): The WiMAX standard uses the Privacy and Key Management Protocol for securely transferring keying material between the base station and the mobile station. The privacy key management (PKM) protocol is responsible for privacy, key management, and authorizing an SS to the BS. The initial draft for WiMAX mandates the use of PKMv1 [6], which is a one-way authentication method. PKMv1 requires only the SS to authenticate itself to the BS, which poses a risk for a Man-in-the-middle (MITM) attack. To overcome this issue, PKMv2 was proposed (later adopted by 802.16e), which uses a mutual (two-way) authentication protocol [5]. Here, both the SS and the BS are required to authorize and authenticate each other. PKMv2 is preventing from the following [7]: BS and SS impersonations, MITM attack and Key exchange issue. PKMv2 authentication/authorization method is shown in

Privacy key management: In both IEEE 802.16-2004 and IEEE 802.16e-2005 standards, MAC layer contains a security sub-layer. To protect network services from attacks and to guarantee secure distribution of susceptible data from the base station to his subscriber station, WIMAX applies strong support for authentication, key management, encryption and decryption, control and management of plain text protection and security protocol optimization.

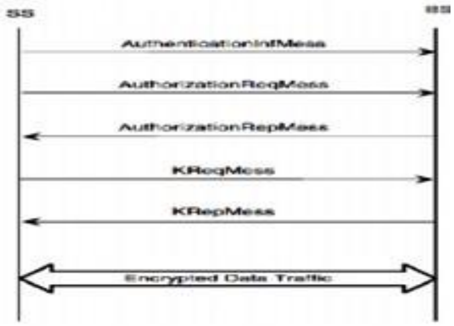

Fig -3: Authentications and Authorization

Subscriber Station (SS) Base Station (BS) Authentication information Authorization Request Authorization Reply Key Request E2E Encryption using TEK Key Reply. PKMv2 supports the use of the Rivest-Shamir-Adleman (RSA) public key cryptography exchange. The RSA public key exchange requires that the mobile station establish identity using either a manufacturer-issued X.509 digital certificate or an operator-issued credential such as a subscriber identity module (SIM) card. The X.509 digital certificate contains the mobile station's Public-Key (PK) and its MAC address. The mobile station transfers the X.509 digital certificate to the WiMAX network, which then forwards the certificate to a certificate authority (Fig-3). The certificate authority validates the certificate, thus validating the user identity. Internet Connectivity Service Network (CSN) WiMAX Access Service Network (ASN) Gateway (GW) A Base Station (BS) Authentication Server Control (R6) Data (IP) Firewall Additional Operator Servers IP network Management System X.509 Digital Certificate Mobile Station (MS) Public-Key Exchange.

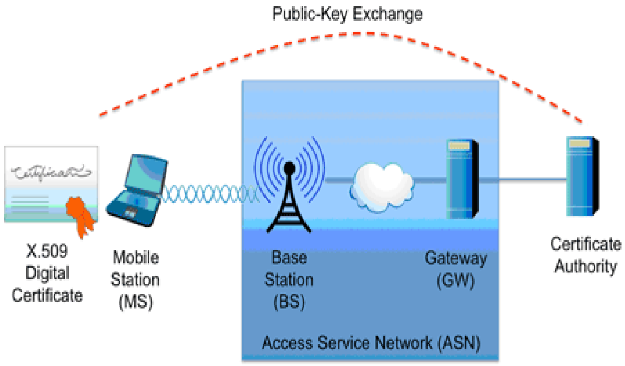

Fig - 4 Public Key Infrastructure

Once the user identity is validated, the WiMAX network uses the public key to create the authorization key, and sends the authorization key to the mobile station. The mobile station and the base station use the authorization key to derive an identical encryption key that is used with the advanced encryption standard (AES) algorithm.

Authentication: Authentication is the process of validating a user identity and often includes validating the services a user may access. The authentication process typically involves a supplicant (that resides in the mobile station), an authenticator (that may reside in the base station or a gateway), and an authentication server (Fig-4).

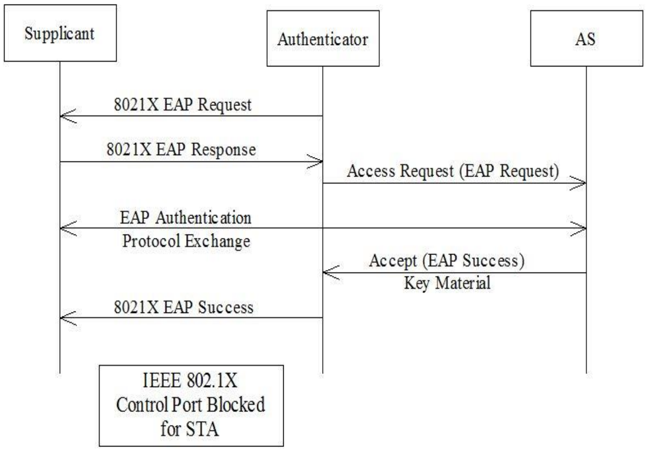

Fig –5: EAP-based authentications

WiMAX uses the Extensible Authentication Protocol (EAP) to perform user authentication and access control are shown in fig-5. EAP is actually an authentication framework that requires the use of "EAP methods" to perform the actual work of authentication. The network operator may choose an EAP method such as EAP-TLS (Transport Layer Security), or EAP-TTLS MS-CHAP v2 (Tunneled TLS with Microsoft Challenge-Handshake Authentication Protocol version 2). The messages defined by the EAP method are sent from the mobile station to an authenticator. The authenticator then forwards the messages to the authentication server using either the RADIUS or DIAMETER protocols [9].

Data privacy and integrity: WiMAX uses the AES to produce ciphertext. AES takes an encryption key and a counter as input to produce a bitstream. The bitstream is then XORed with the plaintext to produce the ciphertext (Fig-6). AES algorithm is the recommendation of 802.16e security sub-layer, since it can perform stronger protection from theft of service and data across broadband wireless mobile network.

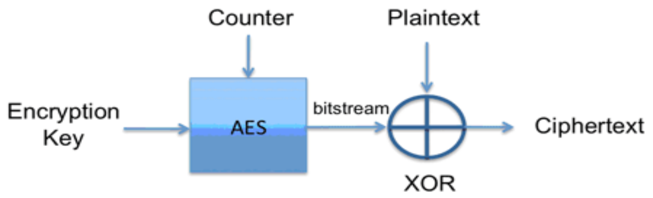

Fig -6: AES Encryption

Besides CCM-Mode and ECB-Mode, AES algorithm supported in 802.16-2004, 802.16e also supports three more AES algorithms: CBC-Mode AES, CTR-Mode AES and AES-Key-Wrap.

Threats and vulnerabilities In WiMAX: Security threats in WiMAX are applicable to both the PHY (Physical) and MAC layers. Possible physical level attacks include jamming of a radio spectrum, causing denial of service to all stations, and flooding a station with frames to drain its battery. Currently, there are no efficient techniques available to prevent PHY layer attacks. Therefore, the focus of WiMAX security is completely at the MAC level [10]. Physical Layer Threats and Vulnerabilities in 802.16 securities are implemented as a sublayer at the bottom of MAC layer in order to protect data exchanged between the MAC layer and the PHY layer. In essence, it does not protect the PHY layer itself against the attacks which target the inherent vulnerability of wireless links. Jamming and scrambling can be the form of attack to the PHY as the WiMAX 802.16 is defenseless. Jamming is achieved by introducing a source of noise strong enough to significantly reduce the capacity of the WiMAX channel. The information and equipment required to perform jamming are not difficult to acquire. Scrambling [10] is similar to jamming but this usually instigated for short intervals of time and is targeted to specific WiMAX frames or parts of frames. WiMAX scramblers can selectively scramble control or management messages with the aim of affecting the normal operation of the network. Slots of data traffic belonging to the targeted SSs can be scrambled selectively, forcing them to retransmit. Another typical attack against the PHY layer, so called water torture attack [6], pushes a SS to drain its battery or consume computing resources by sending bogus frames. This type of attack against a mobile station could be even more destructive than a typical Denial-of-Service (DoS) attack against a wired machine because portable devices are likely to have limited resources. In the mesh mode, 802.16 is also vulnerable to a replay attack in which an attacker maliciously resends valid frames that the attacker has intercepted in the middle of forwarding (relaying) process. The PHY layer attacks can be prevented or mitigated by several trivial countermeasures. Increasing the power of signals can resist jamming attacks. For this, monitoring equipment can be used to detect radio jamming, and upon an abnormal state of radio spectrum the power of signals is increased in order to override malicious signals. The bandwidth of signals can be increased by using spreading techniques such as frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS) [10]. A sophisticated mechanism discarding bogus frames is needed to avoid running out of battery or computational resources by the water torture attack mentioned earlier. The latest 802.16 standard adds support for mobility of SS. This could make 802.16/WiMAX more vulnerable to these attacks against the PHY layer because an attacker does not necessarily have to reside in a fixed point and monitoring the anomaly becomes more difficult. Though intended scrambling is more complex than jamming, the probability for scrambling to occur is possible due to natural noise interruption and the availability periods of the attack. These attacks can be unveiled by analyzing discrepancies in the systems performance.

MAC Layer Threats and Vulnerabilities: There are several significant shortcomings of 802.16 security implemented at the MAC layer. To ultimately set up secure transport connections, 802.16 exploit sequential two-way transactions for controlling, authorization, and authentication. The first problem is that, during the basic and primary connection, MAC management messages are sent in plain-text and not properly authenticated. Thus, the management message can be hijacked over the air and forged by an attacker in the middle. By doing so, the attacker can prepare for further attacks. Secondly, 802.16 uses the X.509 certificate, the standard for PKI that defines a certification path validation to identify a genuine SS. It uses RSA encryption with SHA-1 hashing. Typically, a SS's certificate is pre-configured by the manufacture and persistent on the machine. Thus, the certificate could be stolen and tampered by an adversary unless it is kept secret. Many serious threats arise from its authentication scheme. WiMAX supports unilateral device level authentication [10], which can be implemented in a similar way as Wireless-fidelity (Wi-Fi) MAC filtering based on the hardware device address. Therefore, address sniffing and spoofing make a SS masquerade attack possible. In addition, the lack of mutual authentication makes a MITM attack from a rogue BS possible. However, a successful MITM attack is difficult because of the time division multiple access (TDMA) model in WiMAX. The attacker must transmit at the same time as the legitimate BS using a much higher power level in order to "hide" the legitimate signal. Furthermore, WiMAX supports mutual authentication at user network level based on the generic EAP [11] and its different variants EAP- TLS transport layer security based on X.509 certificate [12] and EAP- SIM [13]. Eavesdropping of management messages is a critical threat for users and a major threat to a system. An attacker could use this vulnerability to verify the presence of a victim at its location before perpetrating a crime. Additionally, it might be used by a competitor to map the network. Another major vulnerability is the encryption mode based on data encryption standard (DES). The 56 bit DES key is easily broken with modern computers by brute force attack. Furthermore, the DES encryption mode includes no message integrity or replay protection functionality and is thus vulnerable to active or replay attacks. The secure AES encryption mode should be preferred over DES [14]. Eavesdropping mostly affects the transfer of information and rarely causes system outage. The assessment of the eavesdropping threat is minor to the system but high for the user. Countermeasures for minor threats are not required. The masquerading threat of the BS or SSs is enabled when authentication weaknesses are present. Identity theft and Rogues BS are specific techniques of masquerading. Identity theft is a severe threat to unlicensed services supported by WiMAX [10,15]. A fake device can use the hardware address of another registered device by intercepting management messages over the air. Once succeeded, an attacker can turn a BS into a rogue BS. A rogue BS can imitate a legitimate BS by confusing the associated SSs. Those SSs try to acquire WiMAX services from the rogue BS, resulting in degraded service or even service termination. Only for comparison, the Wi-Fi network employs carrier sense multiple access (CSMA), and thus identity theft has become one of the top security threats. The reason is that the attacker can easily capture the identity of a legitimate access point (AP) by listening to the CSMA process, which readily reveals information on the AP identity. The attacker can then construct a message by using the legitimate AP's identity, wait until the medium is idle, and distribute the malicious message. Finally, there is a potential for DoS attacks because authentication operations trigger the execution of long procedures. For example, a DoS attack could flood a MS with a high number of messages to authenticate. Due to low computational resources, the MS will not be able to handle a large amount of invalid messages, rendering the DoS attack successful. The impact of this attack is classified to the system as only time is affected at that level, but can be high for the user as it causes delays in the system responding to the individual's requests.

6. SECURITY IN WIRELESS WIDE AREA NETWORKS (WWANS)

Wide area wireless networks can be an enormous benefit to corporation because they have the potential to extend the reach of an enterprise application to a staggering proportion of the earth's surface. However this expanded range also increases the vulnerability of the company's devices, applications and data. In order to ensure their viability we must validate the security of this new infrastructure. Today's legacy and emerging Wireless Wide-Area Networks, such as GSM, GPRS,EDGE, UMTS and cdma2000 already include security provisions that are enforced by the mobile terminals and the base stations. However, there are still shortcomings in the security model that can only be addressed with an end-to-end approach.

GSM Security Features:-

- Key management is independent of equipment: Subscribers can change handsets without compromising security.
- Subscriber identity protection: Not easy to identify the user of the system intercepting a user data.
- Detection of compromised equipment: Detection mechanism whether a mobile device was compromised or not.
- Subscriber authentication: The operator knows for billing purposes who is using the system.
- Signaling and user data protection: Signaling and data channels are protected over the radio path.

GSM Mobile Station

- Mobile Station: This consists of Mobile Equipment (ME), Physical mobile device, Identifiers, IMEI (International Mobile Equipment Identity), Subscriber Identity Module (SIM).
- Smart Card containing keys, identifiers and algorithms.
    - Identifiers: It consists of Ki – Subscriber Authentication Key, IMSI – International Mobile Subscriber Identity, TMSI (Temporary Mobile Subscriber Identity), MSISDN – Mobile Station International Service Digital Network, PIN – Personal Identity Number protecting a SIM.

Authentication and Encryption Scheme: The SIM card is used for the authentication in the Cellular Network, which holds different information about the machine, includes i) IMSI, International Mobile Subscriber Identity Module. ii) Phone number. iii) Authentication key Ki. iv) Subscriber-relevant data (e.g. Text Messages and Phone Directory). v) Security algorithms (e.g. A3).

The Authentication Process [2]: - In GSM, the users are first identified and authenticated then the services are granted. The GSM authentication protocol consists of a challenge-response mechanism. The authentication is based on a secret key Ki which is shared between HLR and MS. After a visited MS gets a free channel by requesting BS, it makes a request for its location update to MSC through BSC. The MSC, in response, asks MS for its authentication. Thus in the authentication process, three major actors like MS, MSC/VLR and HLR/AuC are responsible.

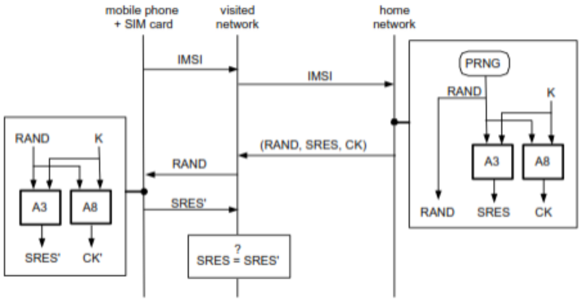

Fig -7: GSM authentication architecture

- The mobile station sends its Temporary Mobile Subscriber Identity (TMSI) to VLR in its request for authentication.
- The MS uses its real identity International Mobile Subscriber Identity (IMSI) when it is switched on for the first time but the temporary identity TMSI is used later.
- The TMSI is used to provide anonymity to the user identity.
- After getting the IMSI of the mobile station from the old VLR using TMSI the VLR sends IMSI to the corresponding HLR/AuC.
- The HLR/AuC uses authentication algorithm (A3) and ciphering key generation algorithm (A8) to create the encryption key (Kc) and Signed Result (SRES) respectively.
- The HLR sends the triplet i.e. Kc, RAND and SRES to VLR.
- The VLR sends the RAND challenge to MS and ask to generate an SRES and send it back.
- The mobile station creates an encryption key Kc and SRES using algorithms A3 and A8 with the inputs secret key Ki and RAND challenge.
- It stores Kc to use it for encryption and sends SRES back to the VLR.

- The VLR compares SRES with the one sent by HLR. If they match, the authentication succeeds otherwise it fails. [2,4,5,6]. It is to be noted that the encryption key Kc is used by both of the parties (home system and mobile station) to encrypt the data and signaling information using A5 algorithm. The encryption is done by mobile equipment not by the SIM because SIM does not have enough power and processing capacity [2,4,5,6].

Overview of the GSM security architecture

- Authentication and key agreement
- Encryption
- Allocation and use of temporary identities

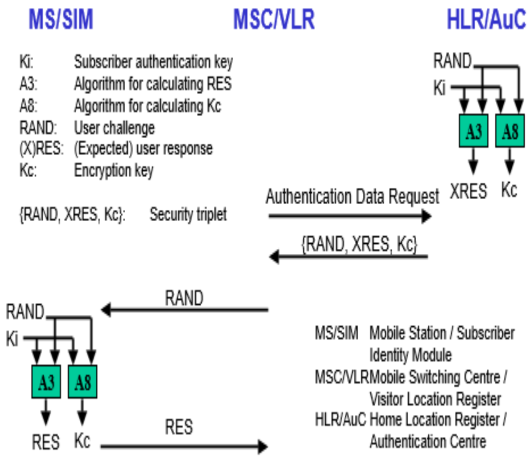
MS/SIM
MSC/VLR
HLR/AuC
Ki: Subscriber authentication key
A3: Algorithm for calculating RES
A8: Algorithm for calculating Kc
RAND: User challenge
(X)RES: (Expected) user response
Kc: Encryption key
{RAND, XRES, Kc}: Security triplet
RAND
Ki
A3
A8
XRES
Kc
Authentication Data Request
{RAND, XRES, Kc}
RAND
RAND
Ki
A3
A8
RES
Kc
RES
MS/SIM Mobile Station / Subscriber Identity Module
MSC/VLR Mobile Switching Centre / Visitor Location Register
HLR/AuC Home Location Register / Authentication Centre

Fig -8: Authentication protocol

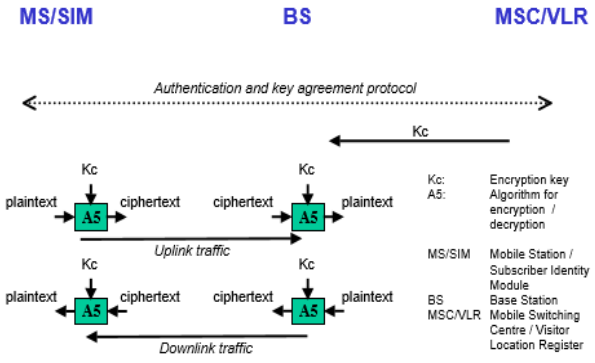
MS/SIM
BS
MSC/VLR
Authentication and key agreement protocol
Kc
Kc
Kc
plaintext
A5
ciphertext
ciphertext
A5
plaintext
Uplink traffic
Kc
Kc
plaintext
A5
ciphertext
ciphertext
A5
plaintext
Downlink traffic
Kc: Encryption key
A5: Algorithm for encryption / decryption
MS/SIM Mobile Station / Subscriber Identity Module
BS Base Station
MSC/VLR Mobile Switching Centre / Visitor Location Register

Fig -9: Encryption

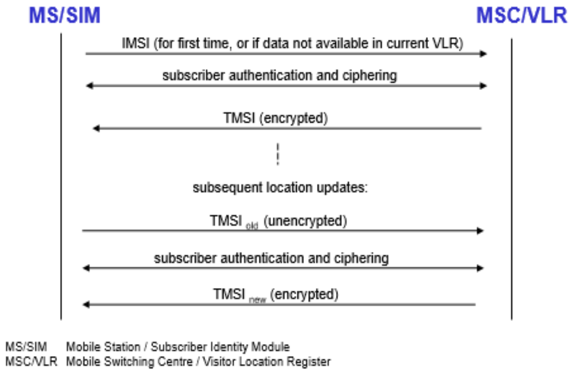
MS/SIM
MSC/VLR
IMSI (for first time, or if data not available in current VLR)
subscriber authentication and ciphering
TMSI (encrypted)
subsequent location updates:
TMSI old (unencrypted)
subscriber authentication and ciphering
TMSI new (encrypted)
MS/SIM Mobile Station / Subscriber Identity Module
MSC/VLR Mobile Switching Centre / Visitor Location Register

Fig -10: Allocation and use of temporary identities

3G Security Principles

It was agreed that any new security architecture must be based on an evolution of GSM and must adopt four basic principles:

- It will take into account the additional features needed for actual or predicted change in the operating environment

- It will maintain compatibility with GSM wherever possible

- It will retain those features of GSM that have proved to be robust and useful to the user and network operator

- It will add or enhance features to overcome actual or perceived weaknesses in 2G system

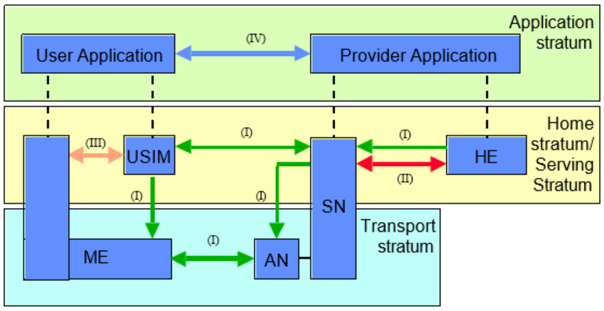

Fig -11: 3G security architecture

Summary of 3G R99 security features (beyond GSM)

- Protection against active attacks on the radio interface: A new integrity mechanism added to protect critical signaling information on the radio interface. Enhanced authentication protocol provides mutual authentication and freshness of cipher/integrity key towards the user.

- Enhanced encryption: Stronger algorithm, longer key-encryption terminates in the radio network controller rather than the base station.

- Core network security: Some protection of signaling between network nodes.

- Potential for secure global roaming: Adoption of 3GPP authentication by TIA TR-45 / 3GPP2.

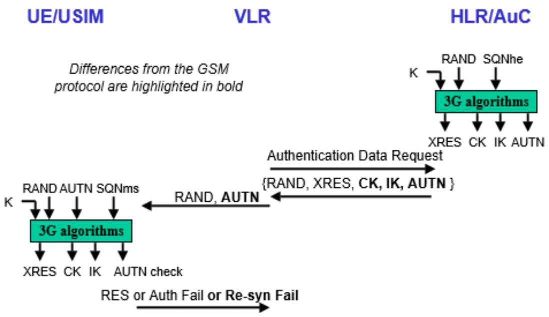
UE/USIM
VLR
HLR/AuC
Differences from the GSM protocol are highlighted in bold
K
RAND SQNhe
3G algorithms
XRES CK IK AUTN
Authentication Data Request
{RAND, XRES, CK, IK, AUTN }
RAND, AUTN
K
RAND AUTN SQNms
3G algorithms
XRES CK IK AUTN check
RES or Auth Fail or Re-syn Fail

Fig -12: Enhance authentication protocol for 3G

4g wireless standards

Previously, the ITU (International Telecommunications Union) defined the IMT-2000 (International Mobile Telecommunications-2000) standard as a global standard for 3G wireless communications. More recently, the ITU embarked on an initiative to define a wireless system beyond IMT-2000 – referred to IMT-Advanced. Work is still underway on standards definition for IMT-Advanced – which may eventually be considered as the formal specification for 4G wireless. The ITU framework and overall objectives for wireless systems beyond IMT-2000 considers both the radio access network (RAN) and the "core network" [1]. 4G wireless technology must support the following criteria:

(a) High data rate (1Gps peak rate for low mobility and 100Mbps peak rate for high mobility)

(b) High capacity

(c) Low cost per bit

(d) Low latency

(e) Good quality of service (QoS)

(f) Good coverage and

(g) Mobility support at high speeds.

In 4G, much effort has been invested in bandwidth optimization and efficiency gain techniques. 4G wireless will also be distinguished by the fact that voice and data will be carried on the same infrastructure utilizing the same set of network protocols. Additionally, the technology should provide a clear evolutionary path to the ITU IMT-Advanced standard for 4G mobile wireless. Several new broadband wireless access technologies have been developed by standards bodies such as 3GPP, 3GPP2, IEEE802.16 & the WiMAX Forum to offer mobile broadband wireless access. Some of these technologies have been labeled as sufficient to meet the requirements for 4G wireless. Initially, candidate technologies for 4G wireless standard included:

- HSPA+ (High Speed Packet Access)
- UMB (Ultra Mobile Broadband)
- LTE
- Mobile WiMAX
- (XGP(eXtended Global Platform)

In reality, only 3 of the 5 technologies were serious considered as candidates for the 4G wireless standard. HSPA+ provides an upgrade over 3G wireless and allows download speeds of 14Mbps to 42Mbps. Many wireless carriers are in the process of evolving their networks to HSPA+ because it requires less investment and time than upgrading to 4G technologies such as LTE. However, HSPA+ technology will not meet the ITU IMT-Advanced requirements of an all-IP interface. Despite the significant bandwidth and performance improvements, it did not meet the stringent ITU requirements for 4G. As a result, the 3GPP-Release 8 LTE standard became the evolutionary path towards 4G for UMTS/HSPA (Universal Mobile Telecommunications System). Another technology under consideration for 4G wireless was the Qualcomm-driven UMB standard. Due to what appeared to be business as opposed to technology related factors, Qualcomm decided to stop working on UMB. XGP is yet another technology described as meeting the 4G wireless requirements. XGP is a 4G upgrade version of the 2G PHS wireless technology which was used by almost 100 million wireless subscribers in Japan/China. While it is possible that XGP may gain momentum within Japan, Asia and a few other countries, PHS represents less than 2% of the global wireless subscriber market. Accordingly, it is not a strong candidate for a global 4G wireless standard.

WiMAX shown in the Fig-13 illustrates the end-to-end network architecture for mobile WiMAX. It consists of two key entities: (i) Access Services Network (ASN) and (ii) Connectivity Services Network (CSN). The core elements in the ASN are the base station (BS) and ASN gateway (ASNGW) which are connected over an IP infrastructure.

The ASN-GW provides security anchoring, traffic accounting and mobility support for the mobile station (MS). The mobile IP home agent (HA) in the CSN enables global mobility. There are a number of key elements in the operation of the WiMAX network architecture. First, the AAA (Authentication, Authorization, and Accounting) server located in the CSN network processes control signals from the ASN-GW to authenticate the MS against the MS's profile stored in the AAA server's database. Once authenticated, the AAA server sends the MS's profile including the QoS parameters to the ASN-GW. The Home Agent (HA) processes control signals from the ASN-GW and assigns a Mobile IP address to the MS and anchors the IP payload. The HA server provides connectivity to the Internet for data traffic.

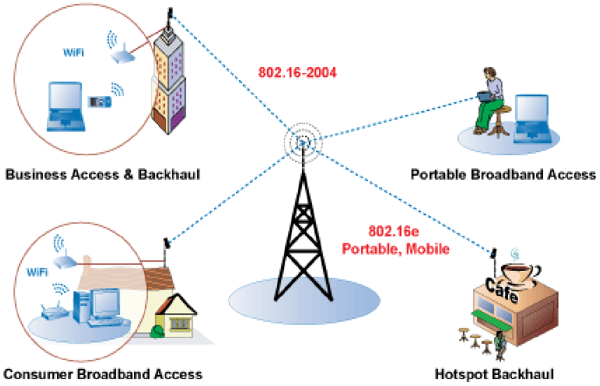
WiFi
802.16-2004
Business Access & Backhaul
Portable Broadband Access
802.16e
Portable, Mobile
WiFi
Cafe
Consumer Broadband Access
Hotspot Backhaul

Fig -13: Mobile WiMAX Network

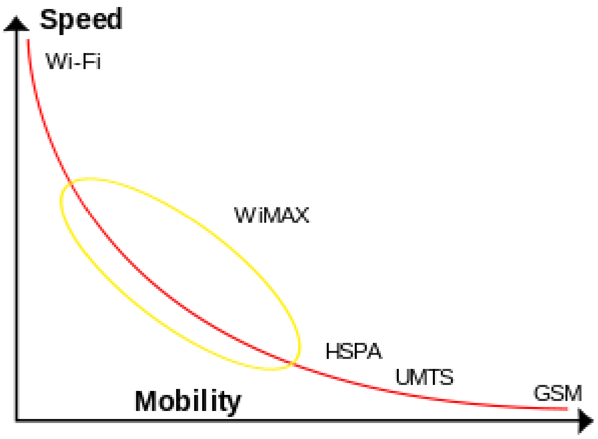

Fig -14: Mobility vs Speed

If the MS makes a VoIP call, control is passed to the CSN IMS (IP Multimedia System) servers which then process the call. If the call is to a telephone number that is outside the WiMAX network, the IMS servers select the appropriate Media Gateway Controller (MGC) / Media Gateway (MGW) to interface to the Public Switched Telephone Network (PSTN). Alternatively, if the call is to an end unit in another 3GPP or 3GPP2 network, it is routed through the Interworking Gateway Unit within the CSN. Mobile Stations (MS) communicate with Base Stations (BS) using the 802.16e (802.16m in the future) air interface. The communication between the MS and BS is via an all-IP bearer and control. WiMAX does not have a TDM (Time Division Multiplexing) bearer. Like LTE, it is an all-IP flat network. WiMAX MS user traffic is tunneled as payload between the BS and ASN-GW. In most service provider configurations, the CSN network elements are redundant and geographically separate. The ASN-GW network elements within the ASN are also configured in a redundant manner typically within the same premises. A Network Access Provider (NAP) can have multiple ASNs. Mobility within these ASNs does not have to be anchored at the CSN. Roaming is supported when the MS roams out of its Home Network Service Provider (NSP) to a Visited NSP. In such cases, the AAA server in the Visited NSP uses control signaling to obtain the credentials and profiles from the Home NSP. Bearer traffic is not sent from the visited NSP to the home NSP. Various mobility scenarios are supported including intra-ASN-GW, inter-ASN-GW and anchored CSN mobility. When the MS moves from one BS to another BS served by the same ASN-GW, calls can be switched seamlessly using signaling.

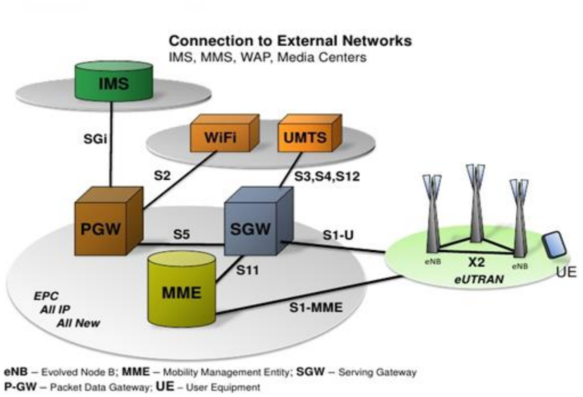
Connection to External Networks
IMS, MMS, WAP, Media Centers
IMS
SGi
WiFi
UMTS
S2
S3,S4,S12
PGW
S5
SGW
S1-U
S11
MME
S1-MME
EPC
All IP
All New
eNB
X2
eNB
eUTRAN
UE
eNB – Evolved Node B; MME – Mobility Management Entity; SGW – Serving Gateway
P-GW – Packet Data Gateway; UE – User Equipment

Fig -15: LTE high level architecture

The UE (user equipment) such as smart phones or laptops connect to the wireless network through the eNodeB within the E-UTRAN (Evolved UMTS Terrestrial Radio Access Network). The E-UTRAN connects to the EPC (Evolved Packet Core) which is IP-based. The EPC connects to the provider wireline IP network shown in the Fig 15.

LTE System Architecture Evolution (SAE): In comparison with 3G wireless, the LTE network architecture has a number of key differences. First, it has fewer types of network elements (NEs). An LTE network consists of 2 types of NEs: (i) the eNodeB which is an enhanced base station (ii) the Access Gateway (AGW) which incorporates all the functions required for the EPC. Second, LTE supports a meshed architecture which allows greater efficiency and performance gains. For example, a single eNodeB can communicate with multiple AGWs. Third, a flat all IP-based architecture is utilized. Traffic originating at a UE is generated in native IP format. These packets are then processed by the eNodeB and AGW using many of the standard functions that are present in IP-based devices such as routers. In addition, the signaling and control protocols for the network are IP-based. The eNodeB (eNB) is the single type of system in the 4G EUTRAN incorporates all the radio interface-related functions for LTE. The AGW is the single type of system in the LTE EPC. The eNB communicates with the UE as well as with the AGW in the EPC. The communication with the AGW occurs over the transport network. Some of the other high level functions carried out by the eNB include (i) inter-cell radio resource management (RRM) (ii) Radio admission control (iii) Scheduling via dynamic resource allocation (iv) Enforcement of negotiated QoS on uplink (v) compression/decompression of packets destined to/from the UE. The AGW consists of multiple modules including the (i) HSS (Home Subscriber Server) (ii) the P-GW (Packet Data Network Gateway) (iii) the S-GW (Serving Gateway) and (iv) the MME (Mobility Management Entity). The LTE standard has sufficient flexibility to allow vendors to combine these different modules into a single device or into multiple devices. e.g. separating the MME and S-GW into different devices. UE data packets are backhauled from the eNB to the AGW over the provider's transport network using IP and MPLS (Multiprotocol Label Switching) networks as the primary vehicle for backhaul in 4G. The MME is the key control-node for the LTE. It is responsible for managing the UE identity as well as handling mobility and security authentication. It tracks the UE while it is in idle mode. The MME is responsible for choosing an SGW for a UE during its initial attach to the network as well as during intra-LTE handover. The MME authenticates the user via interaction with the HSS. The MME also enforces UE roaming restrictions. Finally, the MME handles the security key management function in LTE. The S-GW terminates the interface towards the E-UTRAN. It has key responsibility for routing and forwarding data packets. It acts as the mobility anchor during inter-eNB handovers. The S-GW also has a mandate to replicate packets to satisfy lawful intercept requirements and functions. The P-GW terminates the interface towards the packet data network. i.e. the service provider wireline network. It is the gateway that ultimately allows the UE to communicate with devices beyond the service provider main IP network. UEs may simultaneously connect to multiple P-GWs in order to connect to multiple providers IP networks. Other key functions carried out by the P-GW include (i) Policy enforcement (ii) Per-user packet filtering (iii) billing & charging support (iv) Anchor for mobility between 3GPP and non-3GPP technologies such as WiMAX and CDMA-based 3G (v) Allocating the IP address for the UE. The HSS maintains per-user information. It is responsible for subscriber management as well as for security. The HSS contains the subscription-related information to support network entities handling the calls/sessions. The HSS generates authentication data and provides it to the MME. There is then a challenge-response authentication and key agreement procedure between the MME and the UE. The HSS connects to the packet core based on the IP-based Diameter protocol and not the SS7 (Signaling System Number 7) protocol used in traditional telecommunication networks.

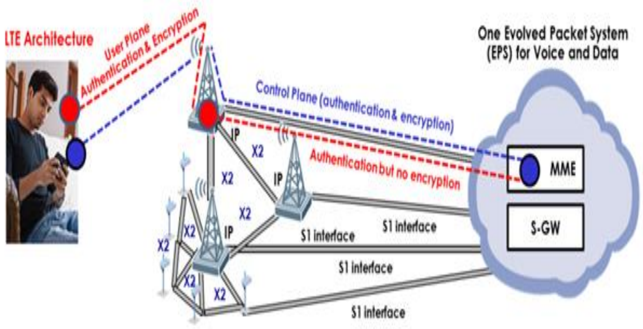
LTE Architecture
User Plane
Authentication & Encryption
One Evolved Packet System
(EPS) for Voice and Data
Control Plane (authentication & encryption)
Authentication but no encryption
MME
S-GW
IP
X2
S1 interface

Fig -16: LTE Encryption

Protecting access to the core network is not enough in LTE networks. As shown in Fig-16, there is a direct path from the eNodeB or small cell directly into the network. If secure access to the core is breached, there is innumerable signaling and bearer paths between core network elements to exploit unless protected internally.
Connection protection can be achieved with an embedded IPsec security gateway in each node. This provides encryption of all control and data plane traffic. An advanced security gateway within the core provides checkpoints to ensure that only truly authorized traffic is passing through the network.

7. CONCLUSION AND FUTURE WORK

In this survey paper, the various issues of security and privacy related to different types of wireless networks like WPAN, WMAN and WWAN are summarized. For each network different security policies are used to avoid different security breaches. For example in WPAN different keys like unit, initialization, combination and master keys are used. In WLAN, WPA2 is the most effective security standard, in WMAN privacy key management(PKM) is used, algorithms like A3, A5 and A8 are used in GSM, 3GPP defines security measures for 3G mobile communication and ASN-GW is used in 4G mobile communications. Further improvements are in progress in wireless security mechanisms to avoid security breaches.

REFERENCES

[1] B. FLECK, J. DIMOV, Wireless access points and ARPpoisoning: wireless vulnerabilities that expose the wired network. White paper by Cigital Inc., (2001). http://www.cigitallabs.com/resources/ papers/download/arppoison.pdf

[2] I. MARTINOVIC, F. A. ZDARSKY, A. BACHOREK, C. JUNG, J. B. SCHMITT, Phishing in the Wireless: Implementationand Analysis. Kaiserslauterer Uniweiter Elektronischer Dokumentenserver, UniversitatsbibliothekKaiserslautern, (2006). http://kluedo.ub.uni-kl.de/volltexte/2006/2035/pdf/martinovic.pdf

[3] G. RUPINDE, S. JASON, C. ANDREW, SpecificationBasedIntrusionDetectioninWLANs.22ndAnnual ComputerSecurityApplicationsConference,Miami Beach, Florida,(2006). 39025942, 60152756p00.htm

[4] L. HAN, A Threat Analysis of The Extensible Authentication Protocol. Honours Project, School of ComputerScience, Carleton University,(2006). http://www.scs.carleton.ca/ barbeau/ Honours/Lei Han.pdf [5] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, FIPS Pub197: Advanced Encryption Standard (AES), (2001).

[6] D. WHITING, R. HOUSLEY, N. FERGUSON, Counter with CBC-MAC (CCM). RFC 3610,(2003).

[7] I. KUMAR, Cryptology. Laguna Hills, CA: Aegean Park Press, (1997).

[8] M. DWORKIN, Recommendation for Block Cipher Modes of Operation – Methods and Techniques. NIST,(2001).

[9] FIPSPUBLICATION197,AdvancedEncryptionStandard (AES). U.S. DoC /NIST, November 26, (2001).

[10] Chip Craig J. Mathias Principal, Farpoint Group COMNET 2003 ―Wireless Security: Critical Issues and Solutions|| 29 January 2003

[11] Sandra Kay Miller ―Facing the Challenge of Wireless Security|| July 2001

[12] T. Karygiannis and L. Owens. Wireless Network Security:802.11, Bluetooth and Handheld Devices. In NIST Special Publication 800-48, November 2002.

[13] Paulo Salvador, Ant´onio Nogueira, Rui Valadas ―Predicting QoS Characteristics on Wireless Networks|| 25 June 2007.

[14] Jim Kurose ―Open issues and challenges in providing quality of service in high-speed networks|| Computer Communication Review, 23(1):6-15, January 1993.