Network Security

Professor Gaurav S. Kasbekar
Department of Electrical Engineering
Indian Institute of Technology, Bombay

Week - 08
Lecture - 46

Wireless Cellular Network Security : Part 4

Hello, recall that in the previous lecture, we discussed UMTS security. In this lecture and the next few lectures, we will discuss the security of 4G networks. In particular, we'll focus on LTE security. LTE stands for Long Term Evolution. It's a popular 4G standard.

We'll discuss its security. The architecture of LTE, which stands for Long Term Evolution cellular networks, is significantly different from that of 2G and 3G networks. So, for 4G, there were a couple of popular standards: one was LTE (Long Term Evolution), and the other was WiMAX. But LTE eventually became more widespread than WiMAX. We'll focus on the security of LTE, which is a 4G standard.

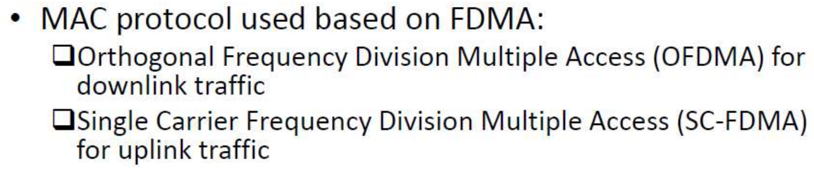
There are several differences between the security in LTE and in 2G and 3G cellular networks. First, we provide an overview of those aspects of the architecture of 2G and 3G cellular networks that we did not discuss earlier but are relevant to 4G networks. Our discussion of 2G and 3G was brief. So, there were some aspects of the architecture of those networks, which we did not discuss, but they are relevant to 4G networks. We'll discuss them now.

Then we'll provide an overview of the architecture of 4G cellular networks. This will help us understand the security of 4G cellular networks later. Once we understand the architecture of 4G cellular networks, we'll then discuss the security in 4G cellular networks. So, first let's discuss the architecture of 4G cellular networks. GSM as well as 3G systems—that is, 2G and 3G systems—were divided into two different domains based on the underlying switching technology.

We have discussed that there are broadly two different switching architectures. One is circuit switching, and the other is packet switching. And GSM and 3G systems had a circuit-switch domain as well as a packet-switch domain. So, the circuit-switch domain was mainly intended for carrying voice and short messages, such as SMSs, and the packet-switch domain was mainly used for carrying data traffic. So, GSM and 3G systems had the circuit-switch domain as well as the packet-switch domain.

And their purposes were these. The circuit-switch domain was for voice and short messages, and the packet-switch domain was for data traffic. In contrast, Evolved Packet System (EPS), which is the technical name for 4G cellular networks, only has a packet-switched domain. So, 4G, based on LTE, has a completely packet-switched architecture. There is no circuit-switched domain in EPS.

The medium access control protocol used is based on FDMA, which we discussed earlier: Frequency Division Multiple Access. In particular, for downlink traffic—that is, traffic which is sent from the base station to the mobiles—the protocol used is OFDMA, which stands for Orthogonal Frequency Division Multiple Access. And for uplink traffic—that is, the traffic from the mobile to the base station—the protocol used is SC-FDMA, which stands for Single Carrier Frequency Division Multiple Access. So, both these MAC protocols are based on FDMA. They are variants of FDMA.



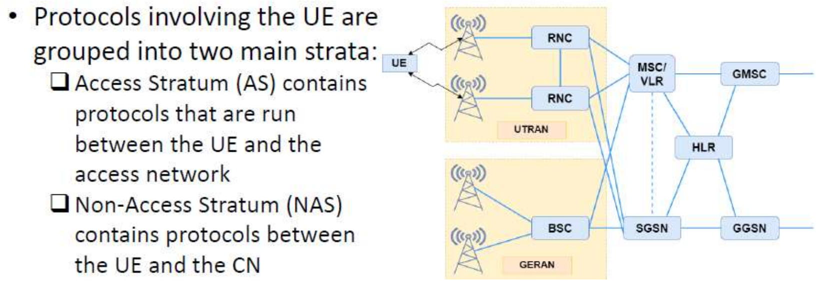
- MAC protocol used based on FDMA:
  - ❑Orthogonal Frequency Division Multiple Access (OFDMA) for downlink traffic
  - ❑Single Carrier Frequency Division Multiple Access (SC-FDMA) for uplink traffic

Different frequency channels are used for different pieces of information. Now, we provide an overview of 3G architecture. This picture illustrates the architecture of 3G networks. This UE is the mobile. UE stands for User Equipment.

It consists of the mobile as well as the SIM card in it. These are the base stations. And this is the BSC, which we discussed earlier: Base Station Controller. One BSC is connected to many base stations. In 3G, the BSC is known by another name: RNC, or Radio Network Controller.

And this is the MSC/VLR which we discussed earlier. This is the GMSC, it is a Gateway MSC which connects the MSC to the telephone network and this is the SGSN which is the counterpart of the MSC in the packet switch part of the network. This is the GGSN which connects the SGSN to the internet and this is the HLR which we discussed earlier, Home Location Resistor. The user equipment or UE, that is the mobile station, is wirelessly connected to the radio access network. The radio access network is shown in this part of the figure. And the radio access network is in turn connected to the core network.

So, this is the core network. This is the core network in the case of 3G. The core network contains a packet switch domain and a circuit switch domain. The packet switch domain is this part consisting of SGSN and GGSN. The packet switch domain is an evolution of the General Packet Radio Service (GPRS) domain of the GSM system.



- Protocols involving the UE are grouped into two main strata:
  - ❑ Access Stratum (AS) contains protocols that are run between the UE and the access network
  - ❑ Non-Access Stratum (NAS) contains protocols between the UE and the CN

So, GSM was a 2G technology and an improvement called GPRS was introduced, which is known as 2.5G cellular networks. So, this added packet exchange features to GSM which was completely circuit switch based. So, using GPRS data packets could be exchanged over the GSM network. So, GPRS is an improvement on the GSM network, which allows internet data to be sent on the network. So, the packet switch domain is an evolution of the GPRS domain of the GSM system and its most important network elements are the SGSN which stands for Serving GPRS Support Node and the GGSN which stands for Gateway GPRS Support Node.

So, these are shown here in the lower part of the figure: SGSN and GGSN. The circuit-switch domain is shown in the upper part of the figure. So, the circuit-switch domain is an evolution from the original circuit-switch GSM network, and the Mobile Switching Center (MSC) is its most important component. So, the MSC is shown here. The protocols that involve the user equipment are grouped into two main strata.

In particular, the Access Stratum (AS) contains protocols that run between the UE and the access network. So, these protocols—the AS protocols—run between the UE and the radio access network, which is the base stations. So, the Access Stratum is the set of protocols that run between the UE and the base stations, whereas the Non-Access Stratum (NAS) contains protocols between the UE and the core network. So, for these non-access stratum protocols, the base station and the BSC or the RNC, they act as relays. And these protocols run between the UE and the core network, which is this.

The CN is further divided into the home network, which contains all the static information about the subscribers, including the static security information. It contains, in particular, keys such as the secret key K_i, which we discussed in the case of 2G and 3G networks. In the case of 4G as well, there will be similar secrets. When we get to 4G security, we will discuss those. So, the key K_i in the case of 3G security is stored in the home network.

We discussed that K_i is stored in the MSC/HLR as well as in the SIM card. So, K_i is in particular stored in the MSC/HLR. So that is shown over here. The other component of the core network is the serving network which handles the communication to the UE via the access network. So, the MSC/VLR is a part of the serving network.

For example, the home network of a subscriber may be Mumbai and the subscriber may be roaming around in Bangalore. So, the serving network is the network in Bangalore. The UE consists of two parts. One is the mobile equipment, that is the mobile phone, and the other part is Universal Subscriber Identity Module (USIM). So, this is the technical name for the SIM card in the case of the 3G networks.

There are two types of radio access networks in the 3G system, which are shown here. This is the first type, and this is the second type. So, one type is UMTS Terrestrial Radio Access Network (UTRAN) that is shown here. It is based on WCDMA technology, that is a 3G technology. CDMA stands for Code Division Multiple Access.

It is a kind of MAC protocol which is used in 3G networks. And the other type of radio access network in the 3G system is GSM/EDGE Radio Access Network (GERAN). It is an evolution of the GSM technology. So that is shown over here. So, there are these two types of radio access networks in the 3G system.

The base station is called node B in the case of UTRAN and Base Transceiver Station (BTS) in the case of GERAN. So, we used the term BTS earlier but it is also equivalently referred to as node B. So, in the case of UTRAN it is referred to as node B, and in the case of GERAN it is referred to as BTS. The base station is connected to the controlling unit of the radio access network and this controlling unit is the Radio Network Controller (RNC) in UTRAN that is shown over here. So, this RNC is the controlling unit of these base stations and the base station controller in the case of GERAN. So that is shown over here.

So, the base station is connected to either the RNC or the BSC. In this picture, these base stations are connected to the RNCs and these base stations are connected to the BSCs. In the core network, the most important element in the circuit switch domain is the switching element MSC, which is shown over here. This is the MSC/VLR and there are many MSCs in the network and the MSC/HLR is also one of them. So, this is the HLR in this figure.

The MSC is typically integrated with a visitor location register that contains a database of the users currently in the location area controlled by the MSC. So, the MSC has a home location register for subscribers in the same area and visitor location register for subscribers who are roaming in that area. The Gateway Mobile Switching Center (GMSC) which is shown here, it takes care of connections to the PSTN or Public Switched Telephone Network. So, this GMSC connects the MSC to the telephone network. In the packet switch domain, the role of MSC/VLR is taken by the SGSN that is shown over here.

So, this is the counterpart of the MSC in the packet switch domain. And the GGSN takes care of connecting to the internet. So, this GGSN is similar to the GMSC. It connects the SGSN to the internet. So, the internet is here.

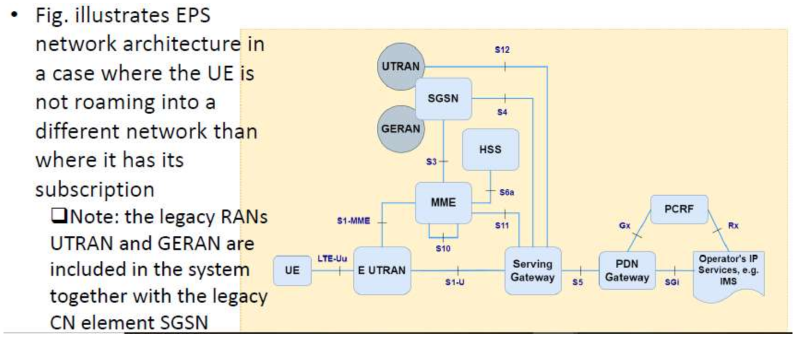
Static subscriber information is maintained in the Home Location Register (HLR), which is here in the figure. The HLR is typically integrated with the Authentication Center (AuC) that maintains the permanent security information related to subscribers. Now, we discuss EPS. That is the 4G system. The goals of the EPS are the following.

One is higher data rates or throughput. Then, lower latency, a higher level of security, enhanced quality of service (QoS), and capabilities for interworking with legacy systems. So, EPS or 4G systems can interwork with 3G and 2G systems. The main means to achieve these goals are the following. One is the new radio interface and the new radio access network based on it, that is, enhanced UTRAN.

And another is a flat IP-based architecture that only has two network elements on the user plane. These elements are evolved NodeB (eNB) and the serving gateway. So, the base station is referred to as eNB or evolved NodeB in the case of 4G. We discussed that in the case of 3G, it is referred to as NodeB. So, evolved NodeB is an evolution of NodeB.

And it is another name for the base station in the context of 4G. This figure illustrates the EPS network architecture, in the case where the UE is not roaming into a different network than where it has its subscription. So, this is the UE; it is connected to the radio access network, which is referred to as enhanced UTRAN in the case of 4G. And this Mobility Management Entity is the MME. So, we'll see that it is responsible for security; that is, the authentication between the UE and the network is performed by the MME.

It is a control plane element and this HSS is an evolution of the HLR or Home Location Register. So, this HSS is the counterpart of HLR in the case of 4G networks. And SGSN we have discussed earlier and this is the UTRAN and GERAN which are connected to the network as well. This is the serving gateway. So, we have seen that the serving gateway is one of the elements in the core network.



- Fig. illustrates EPS network architecture in a case where the UE is not roaming into a different network than where it has its subscription
  - ❑Note: the legacy RANs UTRAN and GERAN are included in the system together with the legacy CN element SGSN

So, this is the serving gateway and it is connected to the PDN gateway which connects the network to the rest of the internet. The legacy RANs, UTRAN and GERAN are included in the system together with the legacy core network element, SGSN. So, these are the legacy radio access networks, UTRAN and GERAN, which we saw in the previous figure. And the legacy core network element SGSN is also included in the same figure. In EPS, there is a new core network element called Mobility Management Entity (MME) that is shown over here.

So, we'll see later that authentication between the network and SIM card is performed by the MME. The HLR of the original GSM and 3G architecture is extended to the Home Subscriber Server (HSS). This HSS is shown here. It is the counterpart of the HLR in the case of 2G and 3G networks. The core network element for user plane handling is called a serving gateway.

So that is shown here. The data packets that are exchanged between the UE and the network flow through the serving gateway and the serving gateway is responsible for these user plane data messages. The Packet Data Network (PDN) gateway, that is shown here handles the traffic towards the packet data networks, such as the internet. So, this PDN gateway handles the traffic towards the PDN which is packet data networks, such as the internet which is on the right of the figure. The core network of the EPS is called Evolved Packet Core (EPC).

So, the architecture of the enhanced UTRAN is depicted in this figure. These are different base stations. As we have seen, they are referred to as eNodeBs in the case of 4G, and these eNodeBs are connected to the core network, and these are core network elements, MME, and serving gateway. So, these blocks shown here, these may be either MMEs or serving gateways. So, often they are combined into one block, so the MME and serving gateway are combined into one unit, which is connected to the base stations.

So, eNodeB is the only type of network element in the enhanced UTRAN. This is an example of an enhanced UTRAN that is a radio access network. It only has base stations. That is the only kind of element in the radio access network. So, it's a very simple architecture.

There is an interface between two eNodeBs which facilitates fast handovers between different base stations. This interface is shown here. This is known as the X2 interface. The X2 interface connects two different eNodeBs. This X2 interface is used for performing handovers, that is when a mobile moves from the range of one base station to the range of another base station, then resources have to be assigned in the new base station to that mobile and resources have to be unassigned from the previous base station.

So, this is performed as part of the handover process and for enabling the coordination between the two base stations, which is done as part of handover, this X2 interface is used. Thus, we can see that there is an X2 interface between each pair of neighboring base stations. There are also connections between the base stations and the core network, known as the S1 interface. These are S1 interfaces between the base stations and the core network. This is the enhanced UTRAN architecture.

In summary, we provided an overview of the 4G network architecture. We saw that it is compatible with 2G and 3G networks as well. We saw a typical network architecture in which the 4G network was connected to 2G and 3G networks. And we saw that there are different parts of the 4G network, including the enhanced UTRAN and the core network, and we discussed their architecture. In the next lecture, we'll begin our discussion on LTE security.

Thank you.