Network Security

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

Week - 08

Lecture - 43

Wireless Cellular Network Security : Part 1

Hello, all of us use wireless cellular networks for getting phone and internet connectivity throughout a city, town, and so on. In this lecture and the next few lectures, we'll discuss the security of wireless cellular networks. We'll first discuss the security of 2G networks, then 3G, 4G, and finally 5G cellular networks. So, cellular networks such as 2G, 3G, 4G, and 5G networks provide internet and telephone connectivity in mobile phones as well as other devices such as laptops and so on, throughout a large region such as a city. Depending on which cellular network standard we use, the speed typically varies from a few tens of Mbps to several Gbps.

So, the 5G standards provide several Gbps of bandwidth. So, these networks operate using the wireless medium, which is a shared medium. That is, when the signal is transmitted, it reaches all the other nodes in the vicinity. So, a MAC protocol, that is, a medium access control protocol, is required to share the available bandwidth among the users in the network. So, different MAC protocols are used in different cellular network standards, 2G, 3G, 4G, and 5G networks.

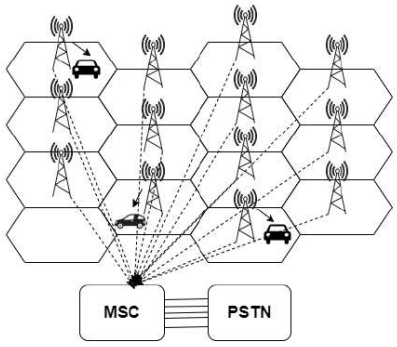
So, these cellular networks are deployed by cellular operators such as Airtel and Vi. And spectrum needs to be licensed from a regulator. So, it is expensive to license out spectrum because the operator needs to participate in an auction and purchase and license out spectrum from the regulator. So, it is expensive, but the advantage is that the access is exclusive for the operator who obtains the license. That is, for example, if an operator acquires a license for 20 megahertz in a particular region, then no other operator is allowed to use those bands. So, using this exclusive access, these operators can provide quality of service guarantees, such as delay guarantees and so on.

So, this picture shows the architecture of a wireless cellular network. The region in which connectivity is to be provided, such as a city, is divided into small areas called cells. In this

picture, each hexagon is a cell. The typical cell radius is less than 5 kilometers. There are cells of various sizes.

It may be in older generations, the cell radius was around a few kilometers. And now there is a, in newer generations of cellular networks, they also use small cells, which have radii of a few hundreds of meters. That helps in increasing the capacity of these networks. So, each cell is served by one base station. For example, the users in this cell are served by this base station, and the users in this cell are served by this base station, and so on and so forth.

So, each cell is served by one base station. As shown in this picture, all the base stations are connected to a node known as MSC, Mobile Switching Center. This architecture is that of a 2G cellular network. This MSC is connected to the public switched telephone network. In modern cellular networks such as 3G, 4G, and 5G, this node is also connected to the internet in addition to the telephone network.

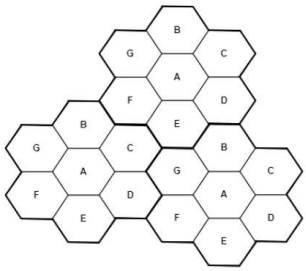


- Region (*e.g.*, city) divided into small areas called *"cells"*
  - ❑typically cell radius < 5 km

So, this node provides connectivity to the telephone network for these base stations. So, for example, calls to users are routed through the base station and through this MSC. So, that way, users can communicate with other users who are connected to the telephone network. Now, what is the reason for breaking the region into small areas called cells? Why not have just one base station at the center of the region that serves the entire region?

So, the reason for breaking the area into small areas called cells is that it increases the capacity of the system through a concept known as frequency reuse. So, the amount of spectrum that is available to an operator is typically limited. For example, 20 MHz may be available to an operator. So, to increase the capacity in terms of the number of users that

can be supported, the same set of frequencies are used in far-apart cells without mutual interference. So, that is illustrated in this picture.



- *Same set of frequencies used at far-apart cells without mutual interference*

Each hexagon is a cell. And the available spectrum with the operator is broken into these parts: A, B, C, D, E, F, G. So, there are seven parts. So, the spectrum is broken into seven parts. So, the overall spectrum, or the available channel, is broken into seven subbands. And these are labeled as A, B, C, D, E, F, G.

And band A is used in this cell and this cell, which is far from this cell, as well as in this cell, which is far from this cell and from this cell, and so on. So, the same frequency bands are used over and over again at mutually far apart locations. The idea is that consider the wireless transmissions from this base station. By the time these wireless transmissions reach this point, their power has attenuated significantly. So, hence, there is very little interference between this cell and this cell, which use the same frequencies.

So, that allows us to use the same frequencies at mutually far apart locations such as these. So, using this concept, the capacity of the system in terms of the number of simultaneous calls or the number of users, the number of subscribers that can be supported, the system increases through this concept of frequency reuse, and that's the reason for breaking the area into small regions called cells, and hence the name cellular networks. Now we start with a discussion of the security in 2G and 3G cellular networks. Later we'll discuss the security of 4G and 5G networks. So, one of the most popular second-generation or 2G cellular networks is GSM, which stands for Global System for Mobile communications.

GSM provided several advantages over analog cellular networks or 1G cellular networks. For example, some advantages were that GSM provides better voice quality and higher speeds for data and other non-voice applications, as well as enabling international roaming. From a security viewpoint, GSM was designed to protect against the following attacks.

One was eavesdropping, that is, if an attacker sniffs the wireless channel between the base station and the mobile, it cannot gain any useful information because the information is encrypted. And if an intruder pretends to be a legitimate mobile phone user, then it cannot connect to the base station because authentication is provided in GSM.

So, GSM defense protects against eavesdropping and intruders pretending to be legitimate mobile phone users. The successor to GSM was UMTS, which stands for Universal Mobile Telecommunication System. It is a 3G technology. So, UMTS provided several advantages over GSM. It provided the following advanced services.

One was mobile internet. So, using mobile phones, one could connect to the internet. It also provided multimedia messaging, video conferencing, and so on. So, UMTS provided these advanced services. The security provided in GSM is significantly better than that in 1G cellular networks.

But GSM security still had several shortcomings, which were overcome in UMTS networks. We'll discuss these shortcomings of GSM security. So, next we study the security mechanisms available in 2G as well as in 3G cellular networks. So, first, let us discuss the architecture of 2G and 3G cellular networks. The architecture is shown in this picture.

So, the overall architecture is divided into the following parts. One is the radio subsystem, and the other is the network and switching subsystem. So, these are illustrated here. The cell phone is wirelessly connected to a base station or base transceiver station. Each hexagon shown here is a cell.

So, we have already seen cells in the previous figures. And each cell, as we have seen before, is served by a base station, and that is known as BTS, or Base Transceiver Station, in GSM terminology. And multiple BTSs are, in turn, connected to and controlled by a Base Station Controller (BSC). We can see here that all these BTSs are connected to this BSC, or base station controller. So, one BSC controls several BTSs.

And the connection between a BTS and its controller, BSC, could be a microwave link or optical link, and so on. So, a microwave link is a wireless link that uses frequencies in the microwave spectrum, or the link could be an optical link that uses fiber optic communication, etc. Multiple BSCs are connected to a Mobile Switching Center (MSC), as shown here. So, all these BSCs are connected to this MSC, which is the mobile switching

center. And different MSCs are connected to each other through the public switched telephone network.

So, this picture shows that all these different MSCs are connected to each other. An MSC forwards an incoming call to the MSC where the call recipient is located. So, for example, a user might be by default located in Mumbai, but the user may be currently roaming around in some other place, say Bangalore. In that case, the MSC of Mumbai forwards an incoming call to the MSC where the recipient is located; that is, Bangalore. The MSC also handles call billing and accounting functions.

MSCs are connected to each other through wired networks such as the Packet-Switched Telephone Network (PSTN). So, these MSCs are connected to each other through the telephone network. And this also shows some other elements, such as HLR, which stands for Home Location Register, and VLR, which stands for Visitor Location Register. So, we'll discuss these later. A user's home network is the one with which the user has a subscription.

For example, if a user is by default in Mumbai, then the user's home network will be the Mumbai MSC. And a network is the part of the overall network managed by a particular MSC. So, here, when we say network, we mean it in a very specific sense. It's the part of the overall cellular network that is managed by a particular MSC. So, in this example, one network is all these BSCs, BTSs, and so on, which are connected to this particular MSC.

Then, this is another network, the network that is served by this particular MSC. So, that is all of this entire network. The MSC has a database that contains information about each of its subscribers, and this database is called the Home Location Register (HLR). So, that is shown here. This is the HLR corresponding to this MSC, and this is the HLR corresponding to this MSC and this MSC.

And the HLR also has another associated element called the authentication center. So, this HLR includes static information such as the subscriber's mobile number and services subscribed to. And there is a secret key stored in the mobile and known only to the HLR. So, this secret key is used to provide security services. The HLR also contains dynamic information for each of its roaming subscribers.

For example, the current location of the subscriber. So, this dynamic information includes the current location of a subscriber, that is, the cellular network the user may be currently visiting. So, this dynamic information is included in the HLR. A subscriber may avail of

the services of other networks called foreign networks that have a roaming agreement with the subscriber's home network. For example, the subscriber may be by default in Mumbai and may be currently roaming around in Bangalore.

So, in that case, the subscriber avails services of foreign networks that are located in Bangalore, assuming that these have an agreement with the subscriber's home network. Each cellular network also maintains a database of users who are currently visiting that network, together with the list of services that the subscriber is entitled to. This is known as the visitor location register, and it is shown over here. So, this has the list of the subscribers who are currently visiting the network covered by this MSC. 2G technology introduced the idea of a Subscriber Identity Module (SIM) card.

It's a smart card that can be removed from one cell phone and placed in another. So, a particular subscriber can place their SIM in a cell phone and use that cell phone, and later on, the subscriber can remove the SIM from that cell phone and place it in another cell phone and use the other cell phone. So, the identity of the subscriber is associated with the SIM card, not with the cellular phone. The SIM card stores three secrets and performs cryptographic operations involving some of these secrets. So, these three secrets are the following:

One is a unique 15-digit subscriber identification number called the International Mobile Subscriber Identity (IMSI). So, this IMSI uniquely identifies each subscriber. The second secret is a 128-bit subscriber authentication key, or K_i, which is the long-term key used for authentication between the SIM card and the base station, or the MSC. This K_i is known only to the SIM and the HLR of the subscriber's home network, and it is used for authentication between the SIM card and the MSC. The third secret is a PIN known to the phone's owner and used to unlock the SIM.

- The secrets are:
  - A unique 15-digit subscriber identification number called the International Mobile Subscriber Identity (IMSI)
  - A 128-bit subscriber authentication key, K_i, known only to the SIM and the HLR of the subscriber's home network

So, this is intended to prevent stolen phones from being used, but it's a rarely used feature in practice. So, we will not discuss this any further. As we have seen, the IMSI is a unique identifier of the subscriber, and we'll discuss the authentication process in which this long-term key K_i is used for authentication. So, what are the objectives of 2G and 3G security?

So, the main security goals in GSM and UMTS are similar to those in wired networks, which we have discussed previously.

So, these security goals are authentication, integrity, and confidentiality. So, another security objective of 2G and 3G is that they provide user identity confidentiality. That is, an intruder should not be able to find out which subscriber is presently communicating with the network. So, that is user identity confidentiality. One way for an eavesdropper to identify a caller is through the IMSI transmitted by the cell phone when a call is made.

To protect user privacy, GSM requires that the IMSI should be used rarely. For example, during the initial authentication to a foreign network. So, if an intruder is eavesdropping on the channel between the user and the network, in that case, it will get the IMSI if it is transmitted, but the IMSI is only used rarely. For example, during initial authentication to a foreign network. Then what do we use in place of the IMSI?

We use another identifier called the TMSI. It's a temporary identifier. So, the Temporary Mobile Subscriber Identity (TMSI), is assigned to a user. So, this TMSI has limited time validity and that too only within a particular network. So, it's difficult to guess the identity of the user from the TMSI.

When a user changes location and moves to a new network, the user's cell phone will have to be re-authenticated, and a new TMSI is assigned. So, the TMSI for a subscriber keeps on changing with time and when the user moves to a new network. The mapping between a cell phone's TMSI and its IMSI is maintained in the VLR. So, the network can find out which subscriber has a particular TMSI using this mapping between the cell phone's TMSI and IMSI, which is maintained in the VLR. Unlike the IMSI, which is a fixed subscriber ID, the TMSI is a random integer, and its use is temporary.

And the TMSI is used to provide user identity confidentiality. If an eavesdropper is eavesdropping on the channel between the subscriber and the network, in that case, it will only get the TMSI, and from the TMSI, it is difficult to get the IMSI. Hence, the user's identity is protected. Does the use of TMSI instead of IMSI help prevent tracking of cell phone users? So, the other security goals of 2G and 3G are these: message confidentiality, entity authentication, and message integrity.

These are the usual goals that we have been discussing for other protocols such as SSL, TLS, and IPsec. So, we start with confidentiality. User data messages and some signaling

messages need to be kept confidential. Signaling messages are control messages which are used to send some control information. Then, entity authentication is the next goal.

The MSC needs to be sure that the call is built to the person making the call. Also, the caller needs to be convinced that it is talking to the genuine base station. So, this is authentication. It has the usual meaning that the person making the call should be convinced that they are talking to the legitimate base station and vice versa. The base station should be convinced that it is talking to the legitimate subscriber.

Then, the next goal is message integrity. The message integrity of signaling messages exchanged between the cell phone and the base station needs to be achieved. So, an intruder should not be able to modify a message sent by the cell phone and modify it and then send the modified message to the base station. And it should not be able to modify the message sent by the base station and forward it to the cell phone. Also, an intruder should not be able to send messages pretending to be the cell phone or the base station to the other party.

So, this is achieved through message integrity. So, in summary, we introduced the topic of cellular network security. We are discussing the security of 2G and 3G cellular networks. Later, we will discuss the security of 4G and 5G cellular networks as well. So, we discussed the architecture of 2G and 3G cellular networks, and we saw that there are different elements in the architecture, such as MSC, HLR, BTS, BSC, and so on.

In the next lecture, we will discuss the security of GSM or 2G. Thank you.