Introduction to LTE networks:

LTE (Long Term Evolution) is a standard for wireless communication of high speed data for mobile phones and data terminals. It was started as a project by the Third Generation Partnership Project (3GPP) group. It provides data rates of up to 300 Mbps downlink and 170 Mbps uplink. It ensures low data transfer latencies. The digital modulation used for the downlink is orthogonal frequency-division multiple access (OFDMA) and for uplink is single-carrier FDMA (SC-FDMA). It supports at least 200 active data clients in every 5 MHz cell. The core network is changed to an IP-based network. The radio access network it uses is called the E-UTRAN.

The LTE network is comprised of the following three main components.

- **The User Equipment (UE**): The user equipment contains certain modules, namely, mobile termination(handles all the communication function), Terminal equipment(terminates the data streams), universal integrated circuit card(UICC - runs an application known as the Universal Subscriber Identity Module that stores user-specific data)

- **The Evolved UMTS Terrestrial Radio Access Network (E-UTRAN**): The E-UTRAN handles the radio communications between the mobile and the evolved packet core. It has a component called evolved base stations, called eNodeB or eNB which controls all the mobiles in one or more cells.

- **The Evolved Packet Core (EPC):** It is the IP based core network used for both calls as well as data services.

Attacks on LTE networks:

Jamming attack on LTE networks: Jeff Reed, the director of the wireless research group at Virginia Tech, has shown that using cheap equipment you can disrupt the working of a large base station that serves a lot of people. Exploiting the vulnerability that exists in the constant synchronization process between phones to base station it is possible to block data transmissions.

Location leakage: The social networking applications and other applications like voice over LTE generate broadcast paging messages from the network to the device. Since the global unique temporary identifier (GUTI) lasts for a long time (up to three days) and also because the broadcast area for LTE is only 2 km^2, it makes it possible to identify the devices. Facebook triggers paging messages due to incoming messages while WhatsApp triggers it when someone other than the user in the conversation is typing to inform the user of so. These broadcast messages are confined to the cell the device is connected to and therefore, allows an attacker to determine the position of the device within the cell simply by watching the broadcast messages. We are aware of the many ways of finding a user's IMSI number such as using an IMSI catcher. With IMSI and user presence in hand, it's then easy to refine location to a much finer degree by getting users to log into a rogue cell. One way to fix this problem is to change the GUTI often enough so as to make it impossible to associate paging messages with a specific individual. Another thing about the LTE is that LTE's access network protocols incorporate reporting mechanisms that allow the network to recover from failures. As a result, a base station can request a failure report from an LTE device which may contain information like which base stations it has seen and with what signal strengths. If an attacker gets a hold of this then they can use it to pin point the device's location.

Denial of service: Certain TAU (Tracking Area Update) reject messages sent by the network are accepted without any integrity protection. This vulnerability can be exploited to carry out a denial of service attack. When the UE sends a TAU request message to a rogue eNodeB then that rogue eNodeB can decode the message as there is no encryption being performed on it. After this, the rogue base station sends the UE a TAU reject message. For example, if the message sent is EMM cause number 7, "LTE services not allowed", then the UE accepts and changes its status to "EU3 ROAMING NOT ALLOWED". This prevents the UE from connecting to legitimate LTE networks until the USIM is reinserted or the UE is rebooted. This way the attacker can downgrade the UE to use 3G or 2G services and allow them to launch any 3G or 2G known attacks on the device. Another form of DOS attack is to deny all network services. This is done by sending the "LTE and non-LTE services not allowed" reject message. In this case, the UE not only changes its status but also changes its state to "EMM DEREGISTERED". This makes the UE's location unknown to the MME and hence, becomes unreachable for any mobile services. As a result, UE does not attempt to attach to LTE, GSM, or 3G networks for normal services even if networks are available.

References:

https://en.wikipedia.org/wiki/LTE_(telecommunication)
http://www.tutorialspoint.com/lte/lte_network_architecture.htm
http://www.infosecisland.com/blogview/22688-LTE-networks-vulnerable-to-jamming-a-question-of-national-security.html
http://www.theregister.co.uk/2015/10/28/facebook_whatsapp_let_lte_mobes_leak_location_data/
http://arxiv.org/pdf/1510.07563.pdf