Chapter 9

Security for 5G Communications

[1]Georgios Mantas, [2]Nikos Komninos, [1]Jonathan Rodriguez, [1]Evariste Logota and [1]Hugo Marques
1. Instituto de Telecomunicações, Aveiro, Portugal
2. City University London, London, United Kingdom

Abstract

Security recently has become an important issue that needs to be addressed in an era where governments are investing heavily into preventive measures against cyber-crime that includes denial of service attacks, tampering attacks, and eavesdropping attacks among others. These types of malpractice are foreseen as threats in future 5G scenarios, since confidential information will be downloaded, uploaded and processed via the upcoming 5G systems. Furthermore, the emergence of the 5G era requires the integration of multiple existing advanced technologies with innovative new techniques which will result in many security breaches. Thus, in this chapter, we present representative examples of potential threats and attacks against the main components of the future 5G systems in order to shed light on the future security issues and challenges in the upcoming 5G era.

9.1 Introduction

Nowadays, the trend towards ubiquitous computing environment, as envisioned by (Weiser, 1991), has led to mobile networks characterized by continuously increasing demand for high data rates and mobility**.** To address these issues, 5G mobile technology has emerged as the most prominent technology and a lot of effort has been placed on it during the past few years with the vision to be deployed by 2020 and beyond. 5G communications aim at providing big data bandwidth, infinite capability of networking and extensive signal coverage in order to support a rich range of high quality personalized services to the end-users. Towards this direction, 5G communications will integrate multiple existing advanced technologies with innovative new techniques. However, this integration can lead to tremendous security challenges in future 5G mobile networks (Bangerter, 2014).

Particularly, it is expected that a wide spectrum of security issues will be raised in 5G mobile networks due to a number of factors including: a) the IP-based open architecture of the 5G system, b) the diversity of the underlying access network technologies of the 5G system, c) the plethora of the interconnected communicating devices, which will also be highly mobile and dynamic, d) the heterogeneity of device types in terms of their computational, battery power and memory storage capabilities, e) the open operating systems of devices, and f) the fact that the interconnected devices are going to be usually operated by non-professional users in security issues.

Consequently, 5G communications systems will have to address more much stronger threats than the current existing mobile communications systems.

However, despite the fact that the upcoming 5G communication systems will be the target of many known and unknown security threats, it is not clear, which threats will be the most serious ones and which network elements will be targeted most frequently. Since such knowledge is of utmost importance towards the provision of guidance in ensuring security for the next generation mobile communication systems, the objective of this chapter is to present the potential security issues and challenges for the upcoming 5G communication systems.

Following the introduction, this chapter is organized as follows. In section 9.2, we give an overview of a potential 5G communication system architecture based on the current related work on 5G communication systems; in section 9.3, representative examples of possible threats and attacks against the main components of the upcoming 5G systems are presented in order to shed light on the their potential security issues and challenges. Furthermore, mitigation techniques, derived from the literature, for the presented attacks are discussed; finally, in section 9.4 we conclude this chapter.

9.2 Overview of a potential 5G Communication System Architecture

In 5G communications, the adoption of a dense heterogeneous architecture, comprising macrocells and small cells, is one of the most promising low-cost solutions that will allow 5G networks to meet the industry's capacity growth needs and to provide a uniform connectivity experience on the end-user's side (Bangerter, 2014). Based on the latest literature, we consider that a potential 5G communication architecture in a macrocell scale, as it is depicted in Fig.1, will include the Base Station (BS), equipped with large antenna arrays, as well as additional large antenna arrays of the BS geographically distributed over the macrocell network. The distributed large antenna arrays will play the role of small cell access points supporting multiple Radio Access Network (RAN) protocols for a wide range of underlying access network technologies (2G/3G/4G). Moreover, the mobile users in outdoor environment will collaborate with each other to form virtual large antenna arrays. The virtual large antenna arrays together with the distributed large antenna arrays (i.e. small cell access points) of the BS will construct virtual massive MIMO links in the small cells. The small cell access points rely on reliable backhaul connectivity over optical fibers (Wang, 2014; Bangerter, 2014).

Furthermore, the buildings located in the 5G macrocell area will be also equipped with large antenna arrays installed outside of the building. Thus, every building will be able to communicate with the BS of the macro cell directly or with the distributed large antenna arrays of the BS. Besides, in every building, the outside installed large

antenna arrays will be connected via cable to the wireless access points inside the building communicating with indoor users (Wang, 2014).

Additionally, the Home eNode B (HeNB) reference architecture, defined by 3GPP in (3GPP TR 23.830 V9.0.0, 2009; 3GPP TR 33.820 V8.3.0, 2009; 3GPP TS 22.220 V10.10.0, 2012), in order to construct femtocell, is very promising for the upcoming 5G communication networks. It is because HeNB femtocell provides an effective solution to address the increasing demand for data rates. In particular, a HeNB femtocell is a low-power and low-range access point mainly used to provide indoor coverage for Closed Subscriber Groups (CSG). HeNB femtocells offload the macrocell network and provide broadband IP backhaul connection to the mobile operator's network through the subscriber's residential Internet access. A number of HeNB femtocells may be grouped and addressed to a gateway, reducing the number of interfaces linked directly with the mobile operator's core network. This gateway is a mobile network operator's equipment which is usually located physically on mobile operator premises (Wang, 2014; Bilogrevic, 2010; Gins, 2012).

Moreover, the mobile femtocell (MFemtocell) concept described in (Wang, 2014) can be another promising technology for future 5G communications. This concept combines the mobile relay concept with femtocell technology to accommodate high mobility users, such as users in public transport trains, buses, and even private cars. MFemtocells will be small cells installed inside vehicles to communicate with users within the vehicles. Also, large antenna arrays will be installed outside the vehicles to enable communication with the BS of the macrocell directly or with the distributed large antenna arrays of the BS (Wang, 2014).

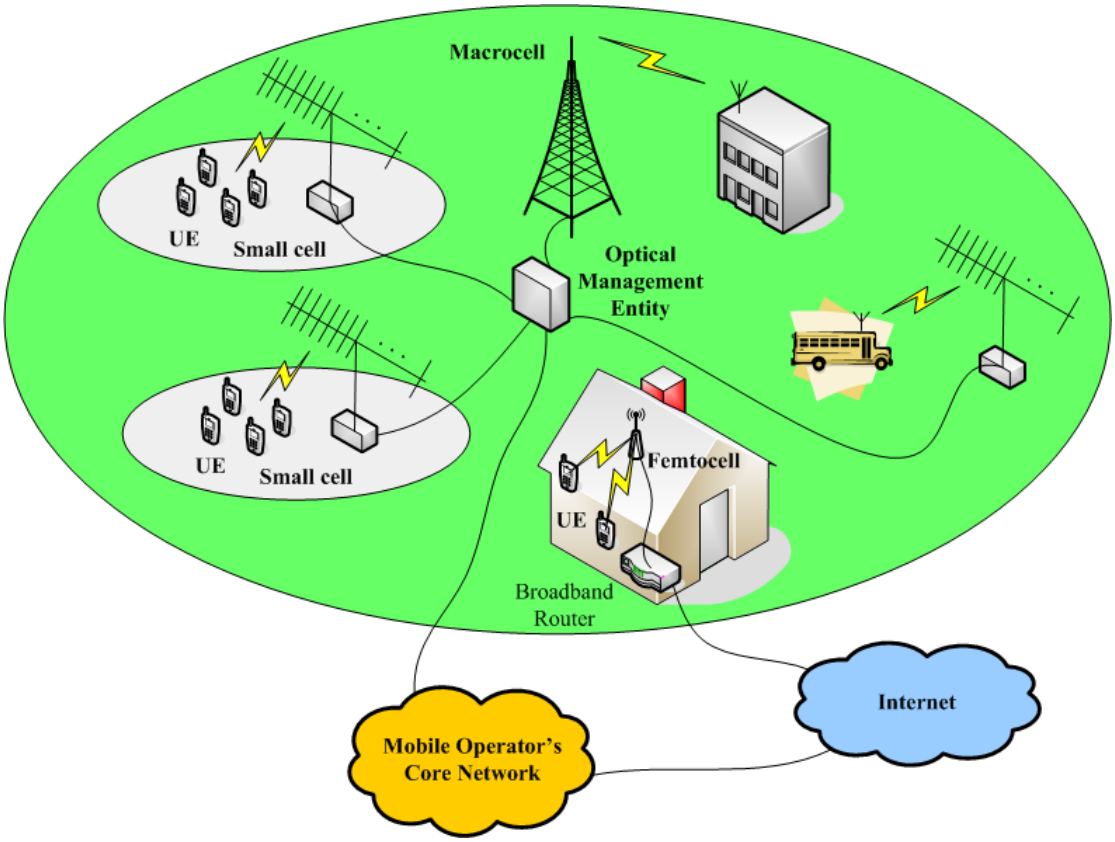

Figure 1. 5G Communication Systems Architecture

9.3 Security Issues and Challenges in 5G Communication Systems

The most attractive targets for future attackers in the upcoming 5G communication systems will be the *User Equipment*, *the access networks*, *the mobile operator's core network* and *the external IP networks*. To help understand the future security issues and challenges affecting these 5G system components, we present representative examples of possible threats and attacks specific to these components. To derive these examples, we explore threats and attacks against legacy mobile systems (i.e., 2G/3G/4G) that can affect the upcoming 5G communication systems by exploiting specific features in this new communication platform. For the presented attacks, we also discuss potential mitigation techniques derived from the literature, in order to provide a roadmap towards the deployment of more enhanced countermeasures.

9.3.1 User Equipment

In the 5G Communications era, User Equipment (UE), such as powerful smartphones and tablets, will be a very important part of our daily life. They will provide a wide range of appealing features to enable end-users to access a plethora of high quality personalized services. However, the expected growing popularity of the future UE combined with the increased data transmission capabilities of 5G networks, the wide adoption of open operating systems and the fact that the future UE will support a large variety of connectivity options (e.g., 2G/3G/4G, IEEE 802.11, Bluetooth) are factors

that render the future UE a prime target for cyber-criminals. Apart from the traditional SMS/MMS-based Denial of Service (DoS) attacks, the future UE will be also exposed to more sophisticated attacks originated from mobile malware (e.g. worms, viruses, trojans) and target both the UE and the 5G cellular network. The open operating systems will allow end-users to install applications on their devices, not only from trusted, but also from untrusted sources (i.e., third-party markets). Consequently, mobile malware, which will be included in applications made to look like innocent software (e.g., games, utilities), will be downloaded and installed on end-user's mobile device exposing them to many threats. Mobile malware can be designed to enable attackers to exploit the stored personal data on the device or to launch attacks (e.g. Denial of Service attacks) against other entities, such as other UE, the mobile access networks, the mobile operator's core network and other external networks connected to the mobile core network. Hence, compromised future mobile devices will not only be a threat against their users, but also against the whole 5G mobile network serving them (La Polla, 2013).

9.3.1.1 Mobile Malware Attacks Targeting UE

As future UE in 5G era will be a personal device storing everything from phone contacts to banking information and taken almost everywhere by the end-user, it will serve as a single gateway to the end-user's digital identity and activities. Thus, the UE will be increasingly vulnerable to mobile malware targeting the stored personal and sensitive information, such as bank credentials, SMSs/MMSs, audio/video files, emails, contacts and GPS coordinates, that attackers can exploit and misuse for financial gain. The malicious software will gain unauthorized access to the stored end-user's information, collect it and forward it to the owner of the malware through all of the UE's communication channels (Becher, 2011; Arabo, 2013; Flo, 2009).

Additionally, the future UE will be vulnerable to mobile malware causing normal service operations disruption. To achieve disruption, the installed malicious software can use all available CPU cycles for junk computations leading to huge power consumption that will rapidly cause the depletion of the UE's power source. This attack falls in the category of Denial of Service attacks against UE (Becher, 2011).

However, the above attacks can be also executed by mobile botnets in order to target many mobile end-users at the same time and in an automated way. Thus, mobile botnets are expected to be a significant means for attackers to gain financial benefits on a larger scale in the 5G era.

9.3.1.2 5G Mobile Botnets

In 5G communication environment, mobile botnets are expected to be increasingly used by attackers, since future mobile devices will be ideal remote controlled machines due to their specific features. In particular, 5G mobile devices will support different connectivity options and increased uplink bandwidth, and will tend to be always turned on and connected to the Internet. Thus, future attackers will be enabled

to deploy mobile botnets for 5G communication networks in many efficient ways (Arabo, 2013; Flo, 2009).

Similar to mobile botnets in legacy mobile networks (La Polla, 2013), future mobile botnets for 5G networks will be networks of compromised mobile devices under the control of malicious actors commonly referred to as bot-masters. For example, a centralized 5G mobile botnet, where the compromised mobile devices will be controlled by the attacker through central Command & Control (C&C) servers, is illustrated in Figure 2. This centralized 5G mobile botnet will consist of the following actors (Arabo, 2013):

- *Bot-master*: will be the malicious actor that can access and manage the botnet remotely via the bot-proxy servers (i.e., central C&C servers). The bot-master will be responsible to choose the mobile devices that will be compromised by malware and turned into bots. Specifically, the bot-master will exploit security vulnerabilities (e.g., operating system and configuration vulnerabilities) of the chosen mobile devices and compromise them. In current mobile botnets, the bot-masters can use similar http techniques, as the PC-based botnets use, as well as new techniques specific to mobile devices' features, such as the SMS messages, in order to distribute their commands. Since 5G UE will support a large variety of connectivity options, it is also possible for the bot-masters of the future 5G mobile botnets to make use of additional techniques in order to command and control their bots.
- *Bot-proxy servers*: will be the means of communication that the bot-master will use to command and control the bots indirectly.
- *Bots*: will be programmed and instructed by the bot-master to perform a variety of malicious activities, such as Distributed Denial of Service (DDoS) attacks against network elements in the mobile network, mass distribution of spam, sensitive data theft and further distribution, as well as installation of malware on other mobile devices.

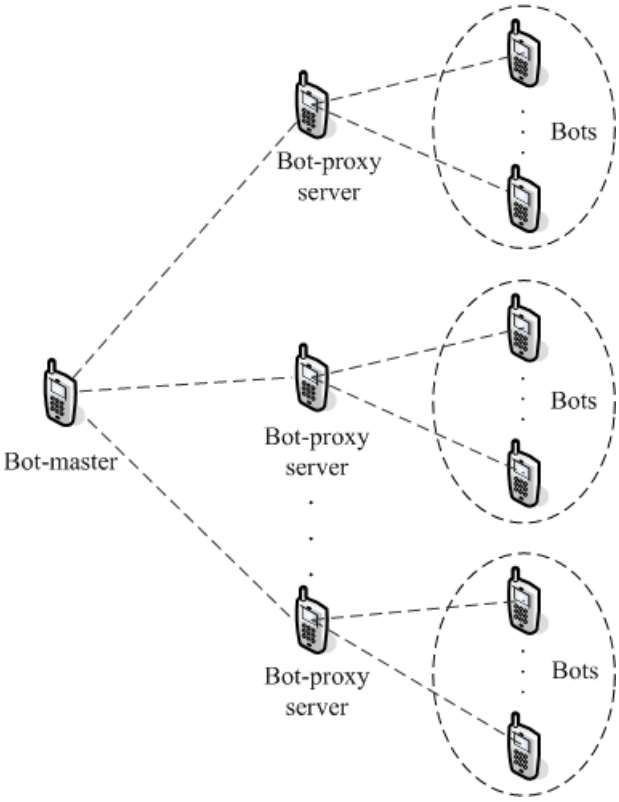

Figure 2. Centralized 5G Mobile Botnet

9.3.2 Access Networks

In 5G communications, access networks are expected to be highly heterogeneous and complex including multiple different radio access technologies (e.g., 2G, 3G, and 4G) and other advanced access schemes such as femtocells in order for service availability to be guaranteed. For instance, in the absence of 4G network coverage, the UE should be able to establish a connection over 2G or 3G networks. However, the fact that 5G mobile systems will support many different access networks leads them to inherit all the security issues of the underlying access networks that they will support (Piqueras Jover, 2013).

During the evolution from 4G communications to 5G communications, enhanced security mechanisms should be implemented to counter emerging security threats on 5G access networks. To address this issue, potential security threats and attacks for the future 5G access networks should be firstly identified. Thus, in this section, we focus on existing attacks on current 4G access networks and HeNB femtocells, which are also deemed possible attacks to the 5G access networks.

9.3.2.1 Attacks on 4G Access Network

In this subsection, we present representative attacks against the 4G access network that can be also expanded to 5G access network. Besides, mitigation solutions addressing these attacks are discussed.

- ***UE Location Tracking***

  Tracking the UE presence in a specific cell or over multiple cells is a security issue for LTE networks that can affect seriously subscriber's privacy. Two techniques that can be used by attackers to achieve UE location tracking in future 5G access networks are those techniques for LTE networks described in (Seddigh, 2010) and (Forsberg, 2007). They are based on the Cell Radio Network Temporary Identifier (C-RNTI) and the packet sequence numbers.

  - *UE Location Tracking based on C-RNTI*

    The C-RNTI provides a unique and temporary UE identification (UEID) at the cell level. It is assigned by the network via a RRC control signal when a UE is associated with the cell. However, the C-RNTI is transmitted in the L1 control signal in plain text. Thus, an adversary is able to determine whether the UE using the given C-RNTI is still in the same cell or not. According to (Forsberg, 2007), periodic C-RNTI re-allocation is a potential solution. Periodic C-RNTI re-allocation for a UE staying for a long time on the same cell can make it more difficult for an attacker to obtain information related to its presence on the cell. Additionally, it will make it more difficult for the attacker to distinguish if indeed a new UE has arrived to the cell or if it is the same UE that refresh its C-RNTI.

    Moreover, UE location tracking can be achieved by tracking the combination of the C-RNTI with handover signals. This combination allows UE location tracking across multiple cells. During the handover process, a new C-RNTI is assigned to the UE via the Handover Command message. Thus, in case that the allocation of C-RNTI itself is not confidentiality protected, an attacker can link the new C-RNTI in the Handover Command message and the old C-RNTI in the L1 control signal (Seddigh, 2010), (Forsberg, 2007). To mitigate this type of attack, encryption of RRC messages, such as the Handover Command message and the Handover Confirm message, is proposed in (Forsberg, 2007). Encryption of these messages prevents an attacker from associating the RRC messages to a C-RNTI and mapping them together during handover processes.

  - *UE Location Tracking based on Packet Sequence Numbers*

    The use of continuous packet sequence numbers for the user plane or control plane packets before and after a handover can enable an attacker to determine the mapping between the old and the new C-RNTIs (Seddigh, 2010). UE tracking based on packet sequence numbers can also be applicable to the idle-to-active mode transitions if the sequence numbers are kept continuous. Then, an attacker can track the UE based on the continuous packet sequence numbers of packet streams. To address UE tracking based on sequence numbers, the

authors in (Forsberg, 2007) propose that the sequence numbers over the radio should be discontinuous in handover processes and possibly also in the state transitions between idle and active modes. Particularly, they propose the use of a random offset in order to make the user and control plane sequence numbers discontinuous on the radio link. Finally, another solution proposed also in (Forsberg, 2007) is the use of fresh keys for each eNB, which allows setting the sequence number to any random value and thus makes it discontinuous.

- ***Attacks based on False Buffer Status Reports***

  In LTE networks, an attacker can exploit the buffer status reports, which are used as input information for packet scheduling, load balancing and admission control algorithms, to achieve his malicious intents. Particularly, the attacker can send false buffer status reports on behalf of the legitimate UE in order to change the behavior of these algorithms on the eNBs and cause serving issues towards the legitimate UE (Forsberg, 2007; Seddigh, 2010).

  By changing the behavior of the packet scheduling algorithm, the attacker is able to steal bandwidth. To achieve that, the attacker can make use of C-RNTIs of other legitimate UE and send false buffer status reports. This can make the eNB consider that the legitimate UE do not have data to transmit. Consequently, the packet scheduling algorithm in the eNB will allocate more resources for the attacker's UE and no or less resources for the legitimate UE. This can lead to denial of service for the legitimate UE.

  Furthermore, by changing the behavior of load balancing and admission control algorithms in the eNBs, denial of service can be experienced by the new arriving UE in the cell. To achieve that, the attacker can send a wide range of false buffer status reports from various UE claiming that they have more data to send than what they actually have. This makes the eNB consider that there is a heavy load in this cell and new arriving UE cannot be accepted.

  To address the attacks based on false buffer status reports, the use of one-time access token within the MAC level buffer status report message is proposed in (Forsberg, 2007). According to this solution, the UE will have to present this token to the eNB to get the access right. The token is different for each buffer status report sent during a Discontinuous Reception (DRX) period.

- ***Message Insertion Attack***

  Message insertion attack is another type of attack for LTE networks and is described in (Forsberg, 2007) and (Seddigh, 2010). In LTE networks, the UE is allowed to stay in active mode, but turn off its radio transceiver to save power consumption. This is achieved through the DRX period. However, during a long DRX period, the UE is still allowed to transmit packets because the UE may have urgent traffic to send. This feature can be a potential security breach. An attacker can inject control protocol data units (C-PDU) to the

system during the DRX period to achieve denial of service attack against the new arriving UE. According to (Forsberg, 2007), a solution for mitigating the message insertion attack is the request for capacity through the uplink buffer status report.

9.3.2.2 HeNB Femtocell Attacks

The physical size, material quality, lower cost components and the IP interface of the HeNB femtocells make them more vulnerable to attacks compared to eNBs (Bilogrevic, 2010). In this subsection, we present the main categories of the potential attacks related to HeNB femtocell, according to (3GPP TR 33.820, 2009), with specific examples of attacks for each category. Additionally, countermeasures for these attacks are discussed. An extensive and detailed list of all possible attacks related to HeNB femtocell and corresponding mitigations can be found in (3GPP TR 33.820, 2009).

- ***Physical Attacks on HeNB***

  Physical tampering with HeNB is an attack where a malicious actor can modify or replace HeNB components. This attack is possible to affect both end-users and mobile operators. For example, modified RF components of a HeNB may interfere with other wireless devices of an eHealth tele-monitoring system in the patient's environment and cause them to malfunction. This can result in health risks for the patient. On the operator's side, a HeNB with modified RF components can impact harmfully on the surrounding macro network. Thus, it is obvious that HeNB should be physically secured in order to prevent easy replacement of its components. In addition, trusted computing techniques should be used to detect when modifications on critical components of a HeNB are occurred. Furthermore, booting HeNBs with maliciously modified software can lead to further security breaches for end-users and operators. This can be achieved in HeNBs supporting user-accessible boot code update methods. As a result, eavesdropping on communication and impersonation towards the network are two possible security issues that end-users have to address. Also, DoS attacks are possible to be launched against the network operators. A mitigation approach is to secure booting process by using cryptographic means, such as a Trusted Platform Module (TPM).

- ***Attacks on HeNB Credentials***

  In this category of attacks, the compromise of HeNB authentication credentials is included. According to this attack, an attacker obtains a copy of the authentication credentials from the wires of the targeted HeNB. Then, any malicious device can use them and impersonate the given HeNB. Thus, the attacker can mount masquerade attacks against the end-user and the operator. The success of obtaining a copy of the credentials of the targeted HeNB is based on the implementation. Consequently, the credentials should be stored

in a protected domain, such as a TPM module, in order for them not to be compromised easily.

- ***Configuration Attacks on HeNB***
  A possible attack of this category is the mis-configuration of the Access Control List (ACL) of the targeted HeNB. Firstly, the attacker gains access to the ACL including the Closed Subscriber Group (CSG) list. Then, he modifies the ACL in order for devices that are not legitimate to access the network. In addition, the attacker can modify the ACL to prevent legitimate devices from accessing the network, as well as to change the level of access for different devices. As a result, legitimate end-users can experience the effects of DoS attacks, and some other malicious end-users can make use of services free of charge if the billing is based on the HeNB. Hence, it is essential to ensure secure creation, maintenance and storage of the ACL.

- ***Protocol Attacks on HeNB***
  Protocol attacks category includes man-in-the-middle attacks on HeNB first network access, which can cause very harmful impact on end-users. HeNBs are vulnerable to this type of attacks when they do not have unique authentication credentials. In these cases, during the first contact of the targeted HeNB to the core network over the Internet, the operator is not able to identify it. Thus, an attacker on the Internet can intercept all traffic originating from the HeNB and get access to private information and exploit it further.
  To address the man-in-the-middle attacks, authentication credentials should be used by the HeNB in the very first contact with the network. The use of UICC or certificates can be potential solutions towards mitigating these attacks. In UICC-based solutions, UICC is inserted in the HeNB by the point of sales or the customer, and mutual authentication between the HSS and the UICC takes place. On the other hand, in certificate-based solutions, the certificate is stored on the HeNB at the manufacturing phase of the HeNB and used for mutual authentication between the first contact node (i.e., Security GW) and the HeNB.

- ***Attacks on Mobile Operator's Core Network***
  Denial of service (DoS) attacks can be launched, through malicious traffic originating from compromised HeNBs, against core network elements. Two categories of DoS attacks which can be directed to the core network, but not to the HeNBs are the following: a) IKEv2 attacks (e.g., IKE_SA_INIT flood attacks, IKE_AUTH attacks) that can be launched against the initial establishment of the IKEv2 tunnel between the HeNB and the Security Gateway, and b) layer 5-7 volume attacks and IKEv2 volume attacks when a high volume of signaling traffic or IKEv2 tunnel setup traffic overwhelms the infrastructure. To mitigate these attacks, Security Gateway should remain secure and available as first contact point in the core network. Furthermore this category encompasses HeNB location-based attacks such as the changing

of the HeNB location without reporting. A malicious actor may relocate the HeNB and make the provisioned location information invalid. As a result, this can cause emergency calls emanating from the relocated HeNBs not to be reliably located or routed to the correct emergency centers. Besides, lawful interception position reporting is impossible. Location locking mechanism is a potential solution to prevent these attacks.

- ***User Data and Identity Privacy Attacks***
  Eavesdropping of the other end-user's E-UTRAN user data is a very harmful attack of this category against the privacy of the end-users. The attacker installs his own HeNB and configures it to the open access mode. Then, the targeted end-user makes use of this malicious HeNB in order to connect to the core network without knowing that this HeNB is compromised. Hence, the attacker is able to eavesdrop all data flowing between the targeted end-user and the network. This attack exploits the unprotected user traffic in some part of the HeNB. For that reason, unprotected user data should never leave a secure domain inside the HeNB to avoid this eavesdropping attack. Furthermore, the end-users should be notified when they are connected to a closed or an open type HeNB.

- ***Attacks on Radio Resources and Management***
  Radio resource management tampering is an attack where the HeNB provides incorrect radio resource information. To achieve this, the malicious actor has to get access to the HeNB and modify the resource management aspects of the HeNB. At least, he should be able to modify the power control part of the HeNB. An example of the consequences with this type of attack can be the increased handover. Thus, the configuration interface of the HeNB should be adequately secured.

9.3.3 Mobile Operator's Core Network

Due to their IP-based open architecture, 5G mobile systems will be vulnerable to IP attacks that are common over the Internet. Denial of Service (DoS) attacks, which are a major threat on the Internet today, are going to be present on the future 5G communication systems targeting entities on the mobile operator's core network. However, the 5G mobile operator's core network can be also affected by Distributed DoS (DDoS) attacks targeting external entities, but transferring their malicious traffic over it. Potential attacks include:

- ***DDoS Attacks Targeting the Mobile Operator's Core Network***
  Distributed Denial of Service (DDoS) attacks will be very serious incidents impacting the availability of the targeted future 5G mobile core network. Since 5G mobile networks are going to be used by millions of users, the consequences of DoS and DDoS attacks against the core network will be severe. In 5G

Communication environment, DDoS attacks can be launched by a botnet including a large number of infected mobile devices. In this subsection, two representative DDoS attacks against the 4G mobile operator's core network are presented. These two examples of attacks can be also expanded to the 5G core network.

- ***Signaling Amplification***

  A DDoS attack example for future 5G mobile operator's core network can be the signaling amplification attack that 4G networks face and is described in (Bassil, 2012). This attack can be performed by a botnet of multiple infected mobile devices within the same cell in order to deplete the network resources leading to service degradation. This attack exploits the signaling overhead required to set up and release dedicated radio bearers in LTE networks. Thus, a large number of dedicated bearer requests will be initiated simultaneously forcing the different network entities to follow the heavy signaling dedicated bearer activation procedure for each bearer. After obtaining the dedicated bearers, the bots will not use them, and after the expiration of the inactive bearer timeout, the bearers will be deactivated following the dedicated bearer deactivation procedure which incurs heavy signaling as well. Then, the malicious devices of the botnet will execute the same steps over and over again to amplify the attack and degrade the network performance. Finally, the proposed detection technique for this attack is based on features such as the inter-setup time and the number of bearer activations/deactivations per minute. The setting of a lower bound threshold for inter-setup time determines the performance of the detection technique. A high value for the inter-setup time threshold would result in too many false positives. On the other hand, a low value for this threshold might lead to undetected exploits. Furthermore, a high number of bearer activations/deactivations per minute indicates malicious activity and should be discovered and stopped by the operator (Bassil, 2012), (Piqueras Jover, 2013).

- ***HSS saturation***

  A potential DDoS attack against the availability of the future 5G mobile operator's core network can be an attack leading to Home Subscriber Server (HSS) saturation, as it is described in (Piqueras Jover, 2013), for 4G networks.

  The HSS is an essential node of the Evolved Packet Core (EPC) since it comprises the master database for a given user and it contains the subscription-related information to support the network entities handling calls/sessions. The HSS also provides support functions in user authentication and access authorization. A Home Network may contain

one or more HSSs based on the number of mobile subscribers, on the capacity of equipment and the organization of the network (EPC, 2014; 3GPP TS 23.002 V12.4.0, 2014). Thus, a DDoS attack against this key node can potentially reduce the availability of the mobile core network significantly.

In (Traynor 2009), some research work has already explored the possibility of overloading a Home Location Register (HLR), which is a key component of the HSS, exploiting a botnet of mobile devices. The results of this research showed that the reduction of the throughput is dependent on the size of the botnet. Moreover, it is worthwhile to mention that in this type of attacks, the legitimate users of the infected mobile devices are unlikely to be aware of their occurrence, since these attacks are executed by quietly launching network service requests and not a flood of phone calls. Finally, according to this research work, basic filtering and shedding are two possible mitigation techniques against such attacks. However, the implementation of mechanisms intelligent enough to respond to more dynamic attacks remains a challenging task. Particularly, it is difficult for a provider to distinguish attacks from other traffic, since a significant amount of context is lost as messages are exchanged between the mobile devices and the HLR (e.g., granularity of location). Furthermore, filtering in the core network may occur too late to prevent legitimate users from experiencing denial of service, due to the large overhead related to the first hop of communications in mobile networks (Traynor 2009).

- ***DDoS Attacks Targeting External Entities over the Mobile Operator's Core Network***

  In future, the upcoming 5G mobile networks can also serve as gateway for DDoS attacks against targets in other external networks (e.g. enterprise networks) connected to the mobile core network. In this scenario, a botnet of mobile devices can be used to generate high volume of traffic and transmit it to the victim, located in the external network's infrastructure over the mobile core network. Although the target of these attacks will not be the core network itself, the fact that they inject large traffic loads into the core network can impact its performance. The recent DDoS attacks against Spamhaus over the Internet proved how the high volume of attack traffic can affect the availability of the underlying communication network employed to transmit it to the specific target (Piqueras Jover, 2013).

9.3.4 External IP Networks

In 5G communication systems, external IP networks can also be the target of DDoS attacks, where mobile botnets generate high volume of traffic and transmit it to the

target over the mobile core network. In addition, external IP networks, such as enterprise networks, can be a soft target for being compromised by malware through infected mobile devices accessing them. In this subsection, we present a representative scenario, based on (Li, 2013), of how an enterprise network can be compromised through the infected 5G mobile device of an employee. Furthermore, a solution against this threat, proposed in (Li, 2013), is also discussed.

- ***Compromised Enterprise Networks***
  The current wide adoption of smartphones has already led many employees to bring their own smartphone devices to the work environment and use them to access information assets located in isolated enterprise networks or enterprise networks with strict access control. This trend is expected to continue and accelerate in the upcoming 5G era. However, many security concerns will be raised for the enterprise networks accessed by employees' smartphones due to the potential susceptibilities of smartphones to mobile malware (Li, 2013). The potential vulnerabilities can be exploited by attackers to compromise an otherwise secure enterprise network. For example, mobile malware, such as Dream Droid (Li, 2013) that recently infected the Android Market, can be used by attackers to get unauthorized access to enterprise networks through employees' future smartphones.

  Furthermore, another characteristic of future employees' smartphones that can be exploited by attackers to compromise enterprise networks will be the diversity of their connectivity capabilities. They will support not only mobile communication technologies (2G/3G/4G/5G), but also other connectivity technologies such as Wi-Fi, Bluetooth, NFC and USB. Thus, the multiple connectivity technologies can be abused by attackers as mobile malware propagation channels. In other words, employees' smartphones can work as bridges for attackers between the enterprise network and the outside world. Thus, an employee's smartphone can be compromised through a mobile communication channel or a short-range communication channel and become a wormhole to the target enterprise network or bring the malicious payload directly to it through another communication channel supported by the smartphone.

  In an attack scenario, we consider that the employee's smartphone is connected to a desktop PC through USB and the desktop PC is connected to the internal enterprise network. Then, the bot-master can be connected to a backdoor on the employee's smartphone via Wi-Fi or the 4G mobile network and inject the malicious payload to the internal enterprise network through the USB connection.

  To avoid security breaches for the enterprise network arising from the use of employees' smartphones inside the work environment, a very common approach is to periodically scan all employees' smartphones with anti-malware software. However, this approach is intrusive and too costly energy-wise. Thus, innovative solutions providing a balance between security responsiveness and cost

effectiveness are required. In (Li, 2013), strategic sampling is proposed as a method to address this requirement by identifying and periodically sampling the security representative smartphones. Then, the sampled devices are checked for malware infections. Smartphones' security representativeness is measured by the employees' interests and the co-location logs on their devices. The probabilities used in the strategic sampling method are derived from a lottery tree reflecting the smartphones' security representativeness (Li, 2013).

9.4 Conclusion

In this chapter, we have presented representative examples of potential threats and attacks against the main components of the upcoming 5G communication systems in order to elucidate the future security issues and challenges in the upcoming 5G era. Particularly, we have focused on examples of potential threats and attacks for the following 5G system components: the UE, the access networks, the mobile operator's core network and the external IP networks. To derive the presented examples, we are based on threats and attacks against current existing mobile communication systems that can be expanded to the next generation 5G communication systems by exploiting their specific features. Finally, we have discussed potential mitigations, derived from the literature, for the presented attacks, since our vision is to provide a roadmap towards the deployment of more enhanced countermeasures addressing properly the potential security issues of the upcoming 5G communication systems.

References

Arabo, A., & Pranggono, B. (2013, May). Mobile Malware and Smart Device Security: Trends, Challenges and Solutions. In *Control Systems and Computer Science (CSCS), 2013 19th International Conference on* (pp. 526-531). IEEE.

Bangerter, B., Talwar, S., Arefi, R., & Stewart, K. (2014). Networks and devices for the 5G era. *IEEE Communications Magazine*, 52(2), 90-96.

Bassil, R., Chehab, A., Elhajj, I., & Kayssi, A. (2012, October). Signaling oriented denial of service on LTE networks. In *Proceedings of the 10th ACM international symposium on Mobility management and wireless access* (pp. 153-158). ACM.

Becher, M., Freiling, F. C., Hoffmann, J., Holz, T., Uellenbeck, S., & Wolf, C. (2011, May). Mobile security catching up? revealing the nuts and bolts of the security of mobile devices. In *Security and Privacy (SP), 2011 IEEE Symposium on* (pp. 96-111). IEEE.

Bilogrevic, I., Jadliwala, M., & Hubaux, J. P. (2010). Security issues in next generation mobile networks: LTE and femtocells. In *2nd international femtocell workshop* (No. EPFL-POSTER-149153).

Flo, A. R., & Josang, A. (2009, October). Consequences of botnets spreading to mobile devices. In *Short-Paper Proceedings of the 14th Nordic Conference on Secure IT Systems (NordSec 2009)* (pp. 37-43).

Forsberg, D., Leping, H., Tsuyoshi, K., & Alanara, S. (2007, September). Enhancing security and privacy in 3GPP E-UTRAN radio interface. In *Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007. IEEE 18th International Symposium on* (pp. 1-5). IEEE.

Gins, E. A., Raphael, C. W. P., & Parish, D. J. Analysis and design of security for next generation 4G cellular networks. In *the Convergence of Telecommunications, Networking and Broadcasting (PGNET2012), 13th Annual Post Graduate Symposium on* (pp. 1-7).

Han, C. K., Choi, H. K., & Kim, I. H. (2009, November). Building femtocell more secure with improved proxy signature. In *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE* (pp. 1-6). IEEE.

Khosroshahy, M., Qiu, D., Ali, M., & Mustafa, K. (2013, August). Botnets in 4G cellular networks: Platforms to launch DDoS attacks against the air interface. In *Mobile and Wireless Networking (MoWNeT), 2013 International Conference on Selected Topics in* (pp. 30-35). IEEE.

La Polla, M., Martinelli, F., & Sgandurra, D. (2013). A survey on security for mobile devices. *Communications Surveys & Tutorials, IEEE*, 15(1), 446-471.

Li, F., Peng, W., Huang, C. T., & Zou, X. (2013, June). Smartphone strategic sampling in defending enterprise network security. In *Communications (ICC), 2013 IEEE International Conference on* (pp. 2155-2159). IEEE.

Piqueras Jover, R. (2013, June). Security attacks against the availability of LTE mobility networks: Overview and research directions. In *Wireless Personal Multimedia Communications (WPMC), 2013 16th International Symposium on* (pp. 1-9). IEEE.

Seddigh, N., Nandy, B., Makkar, R., & Beaumont, J. F. (2010, August). Security advances and challenges in 4G wireless networks. In *Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on* (pp. 62-71). IEEE.

Traynor, P., Lin, M., Ongtang, M., Rao, V., Jaeger, T., McDaniel, P., & La Porta, T. (2009, November). On cellular botnets: measuring the impact of malicious devices on a cellular network core. In *Proceedings of the 16th ACM conference on Computer and communications security* (pp. 223-234). ACM.

Wang, C. X., Haider, F., Gao, X., You, X. H., Yang, Y., Yuan, D., Aggoune, H. M., Haas, H., Fletcher, S., & Hepsaydir, E. (2014). Cellular architecture and key technologies for 5G wireless communication networks. *IEEE Communications Magazine*, 52(2), 122-130.

Weiser, M. (1991). The computer for the 21st century. *Scientific American*, 265(3), 94-104.

3GPP TR 23.830 V9.0.0. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture aspects of Home NodeB and Home eNodeB (Release 9), September 2009.

3GPP TR 33.820 V8.3.0. 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; Security of H(e)NB (Release 8), December 2009.

3GPP TS 22.220 V10.10.0. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service requirements for Home NodeB (HNB) and Home eNode B (HeNB) (Release 10), September 2012.

3GPP TS 23.002 V12.4.0. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Network architecture (Release 12), March 2014.

EPC (2014). 3GPP-The Evolved Packet Core. http://www.3gpp.org/technologies/keywords-acronyms/100-the-evolved-packet-core